US-CERT Cyber Security Bulletin

SB04-133 *May 12, 2004*

Information previously published in CyberNotes will now be incorporated into US-CERT Cyber Security Bulletins, which are available from the US-CERT web site at http://www.us-cert.gov/cas/bulletins/index.html. You can also receive this information through e-mail by joining the Cyber Security Bulletin mailing list. Instructions are located at http://www.us-cert.gov/cas/signup.html#tb.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between April 22 and May 11, 2004. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
3Com[1]	Multiple	3Com Super Stack 3 NBX 4.0.17, 4.1.4, 4.1.21, 4.2.7	A Denial of Service vulnerability exists when an affected port is scanned with a Nessus security audit tool that is configured in safeChecks mode.	No workaround or patch available at time of publishing.	3Com SuperStack 3 NBX Netset Application Port Scan Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a Nessus security scanner.
Adam Webb[2]	Windows, Unix	Nuke-Jokes 1.7, 2.0 Beta	Multiple input validation vulnerabilities exist due to insufficient sanitization of user-supplied input, which could let a malicious user obtain sensitive information, modify information, or execute arbitrary code.	No workaround or patch available at time of publishing.	NukeJokes Module For PHP-Nuke Multiple Input Validation	Medium **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required; however, Proofs of Concepts have been published.
Admin Access With Levels[3]	Multiple	Admin Access With Levels Plug-in 1.5.1	A vulnerability exists in the '/admin' directory, which could let a malicious user obtain administrative access.	The developer of osCommerce responded that "we do not provide support for contributions" and that "contributions are used at own risk."	Admin Access With Levels Plug-in For osCommerce Administrative Access	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[1] Bugtraq, April 29, 2004.
[2] Securiteam, May 9, 2004.
[3] SecurityFocus, April 29, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Aldo's Tools [4]	Windows	Aldo's Web Server 1.5	Two vulnerabilities exist: a Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information; and a vulnerability exists because a remote malicious user can connect to the target service and enter an arbitrary character to cause the web service to disclose the installation path.	No workaround or patch available at time of publishing.	Aldo's Web Server Multiple Input Validation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Apple[5, 6]	Windows 95/98/ME/ NT 4.0/200, MacOS 9 9.0,9.0.4, 9.1, 9.2, 9.2.1, 9.2.2 Mac OS X 10.x	iTunes Player 4.2.72, Quick Time Player 6, 5.0.2, 6.1, 6.5	A vulnerability exists in the 'QuickTime.qts' file due to an integer overflow within a routine used for copying Sample-to-Chunk table entries from the 'stsc' atom data in a QuickTime-format movie (".mov") into an array, which could let a remote malicious user cause a Denial of Service or execute arbitrary code with SYSTEM privileges.	Upgrades available at: http://www.apple.com/quicktime/download/	Apple QuickTime Sample-to-Chunk Integer Overflow CVE Name: CAN-2004-0431	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Apple[7, 8]	MacOS X 10.2.x, 10.3.x	Mac OS X 10.2-10.2.8, 10.3-10.3.3, Mac OS X Server 10.2-10.2.8, 10.3-10.3.3	Multiple vulnerabilities exist: a vulnerability exists in 'CoreFoundation' when handling environment variables, which could possibly let a malicious user obtain elevated privileges (this has not been confirmed though); a vulnerability exists in 'Radmin' because large requests are not handled properly, which could potentially let a remote malicious user compromise the system (this has not been confirmed though) (only affects version 10.2.8); and a buffer overflow vulnerability exists in 'AppleFileServer' due to a boundary error within the password handling, which could let a remote malicious user execute arbitrary code.	Patches available at: http://download.info.apple.com/Mac_OS_X	Mac OS X CoreFounda-tion CVE Name: CAN-2004-0428, CAN-2004-0429, CAN-2004-0430	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
APSIS[9]	Unix	Pound 1.5	A vulnerability exists due to a format string error within the 'logmsg()' function, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.apsis.ch/pound/Pound-current.tgz	Pound Remote Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[4] Bugtraq, May 3, 2004.
[5] Apple Security Bulletin, APPLE-SA-2004-04-30, April 30, 2004.
[6] VU#782958, http://www.kb.cert.org/vuls/id/782958.
[7] Apple Security Advisory, APPLE-SA-2004-05-03, May 3, 2004.
[8] VU#648406, http://www.kb.cert.org/vuls/id/648406.
[9] Secunia Advisory, SA11528, May 3, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Business Objects[10]	Windows 2000, XP	Crystal Reports 10.0	Several vulnerabilities exist in the web interface, which could let a remote malicious user cause a Denial or Service, or view and delete arbitrary files on the target system.	No workaround or patch available at time of publishing.	Business Objects Crystal Reports Multiple Unspecified Vulnerabilities	Low/ Medium (Medium if arbitrary files can be viewed or deleted)	Bug discussed in newsgroups and websites.
Check Point Software[11]	Windows NT 4.0/2000, Unix	FireWall-1 GX 2.0, VSX 2.0.1, VSX NG with Application Intelligence, Next Generation FP3. HF1&2, NG-AI R55, NG-AI R54, Secure Client NG with Application Intelligence R56, Secu Remote NG with Application Intelligence R56, VPN-1 VSX 2.0.1, VPN-1 VSX NG with Application Intelligence	A buffer overflow vulnerability exists in Check Point VPN-1 products in the processing of ISAKMP packets during negotiations of a VPN tunnel, which could let a remote malicious user execute arbitrary code.	Hotfixes available at: http://www.checkpoint.com/techsupport/downloadApp/	VPN-1 ISAKMP Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[10] Bugtraq, May 2, 2004.
[11] Secunia Advisory, SA11546, May 5, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Chris Burge [12]	Windows	Web Server Com-pieuw.1, beta 2, Com-pieuw	A remote Denial of Service vulnerability exists when a malicious user submits a malformed HTTP GET request.	Upgrades available at: http://prdownloads.sourceforge.net/wwwserver/www.zip?download	DiGi WWW Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Cisco Systems[13, 14, 15] ***Updated advisory issued[16]***	**Multiple**	**Cisco IOS 12.x, R12.x**	**A remote Denial of Service vulnerability exists due to an error within the processing of solicited SNMP requests.** ***Cisco has released an update to their initial advisory. The update has expanded on the affected products section (added the Catalyst and Optical products - 12.1(20)EO) as well as the software versions and fixes section.***	**Updates and workarounds available at: http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml**	**Cisco Internet Operating System SNMP Message Processing Remote Denial of Service**	**Low**	**Bug discussed in newsgroups and websites.**

[12] Secunia Advisory, SA11490, April 28, 2004.
[13] Cisco Security Advisory, 50980, April 23, 2004.
[14] VU#162451, http://www.kb.cert.org/vuls/id/162451.
[15] TA04-111B, http://www.us-cert.gov/cas/techalerts/TA04-111B.html.
[16] Cisco Security Advisory, 50980 Revision 1.5, May 5, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Citrix[17]	Windows NT 4.0/2000, XP, 2003	Meta Frame for Microsoft Windows 2000 1.8, Meta Frame for MS NT 4.0 Server Terminal Server 1.8, Meta Frame XP for Microsoft Windows 2000 1.0, 2003 1.0, XP for MS NT 4.0 Server Terminal Server 1.0, XP Presenta-tion Server for Windows 1.0	A vulnerability exists because a remote authenticated malicious administrator can run a specially crafted program to access a target user's client drives via the target user's ICA connection.	Updates available at: http://support.citrix.com/kb/entry.jspa?entryID=4289&categoryID=118	MetaFrame Presentation Target User's Client Drives	Medium	Bug discussed in newsgroups and websites.
David Collier-Brown[18] ***OpenPKG issues advisory***[19]	**Unix**	**ssmtp 2.50.6**	**Two vulnerabilities exist due to format string errors within the 'die()' and 'log_event()' functions, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code.**	**Debian:** **http://security.debian.org/pool/updates/main/s/ssmtp/** ***OpenPKG:*** **ftp://ftp.openpkg.org/release/2.0/UPD/ssmtp-2.48-2.0.1.src.rpm**	**SSMTP Mail Transfer Format String Vulnerabil-ities**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**
David Stes[20]	Unix	IPMenu Netfilter/ IPtables Rule Editor .1, Editor .2, Editor .3	A vulnerability exists because the '/tmp/ipmenu.log' temporary file is created in an unsafe manner, which could let a remote malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	IPMenu Unsafe 'ipmenu.log' Temporary File	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[17] cqure.net Security Vulnerability Report, 20040430, Ap ril 30, 2004.
[18] Debian Security Advisory, DSA 485-1, April 14, 2004.
[19] OpenPKG Security Advisory, OpenPKG-SA-2004.020, May 7, 2004.
[20] SecurityTracker Alert, 1010064, May 4, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Delegate.org [21]	Windows 95/98/ME/ NT 4.0/2000, Unix	DeleGate 7.7 .0, 7.7.1, 7.8.0-7.8.2, 7.9.11, 8.3.3, 8.3.4, 8.4.0, 8.5.0, 8.9-8.9.2	A buffer overflow vulnerability exists due to a boundary error within the 'ssl_prcert()' function in the SSLway filter, which could let a remote malicious user execute arbitrary code.	Upgrades available at: ftp://ftp.delegate.org/pub/DeleGate/download.html	DeleGate SSLway Filter Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
e107.org[22]	Windows, Unix	e107 website system 0.6 10-0.6 14, 0.545, 0.554, 0.555 , 0.603	A vulnerability exists in 'news submit' and 'article submit' due to insufficient validation, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrades available at: http://prdownloads.sourceforge.net/e107/e107v0.615.tar.gz?download	e107 Website System Multiple Script HTML Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Eight-fifteen Studios[23]	Windows	efFingerD 0.2.12	A buffer overflow vulnerability exists in the 'sockFinger_DataArrival()' function when handling overly long arguments, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	EFFingerD Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
e-Zone Media Inc.[24]	Windows NT 4.0/2000, Unix	FuseTalk 2.0	Multiple vulnerabilities exist: a vulnerability exists in 'banning.cfm' due to a failure of the application to properly validate authentication credentials, which could let a remote malicious ban arbitrary hosts from accessing the affected forum by flagging their IP address; a vulnerability exists in the 'adduser.cfm' script because it is possible to add users via a 'GET' request, which could let a remote malicious user execute arbitrary code; and multiple Cross-Site Scripting vulnerabilities exist, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	FuzeTalk Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[21] 0xbadc0ded Advisory #03, May 6, 2004.
[22] Secunia Advisory, SA11567, May 8, 2004.
[23] Secunia Advisory, SA11573, May 10, 2004.
[24] Secunia Advisory, SA11555, May 6, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Francisco Burzi[25]	Windows, Unix	PHP-Nuke 6.0, 6.5, RC1-RC3, 6.5 FINAL, BETA 1, 6.6, 6.7, 6.9, 7.0 FINAL, 7.0, 7.1, 7.2	Multiple SQL vulnerabilities exist in the 'modules.php' module, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHPNuke Multiple SQL 'Modules.php'	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Francisco Burzi[26]	Windows, Unix	PHP-Nuke 7.2	Multiple SQL injection vulnerabilities exist in the Video Gallery Module due to insufficient sanitization of user-supplied input prior to using it in an SQL query, which could let a remote malicious user obtain unauthorized access to sensitive information.	No workaround or patch available at time of publishing.	PHP-Nuke Multiple Video Gallery Module SQL Injection	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, Proof of Concepts have been published.
Fredric Fredricson [27]	Unix	P4DB Reposi-tory Web Interface 0.99 h-2, 2.0 1, 2.0	Multiple vulnerabilities exist in various scripts due to a failure to validate user-supplied input before it is used in various functions or returned to the user, which could let a remote malicious user execute arbitrary HTML or script code.	It has been reported that the developer of this software has discontinued support for this application.	P4DB Multiple Input Validation	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Greg Wettstein [28, 29]	Unix	Sysklogd 1.1-1.4.1	A remote Denial of Service vulnerability exists because 'sysklogd' does not allocate enough memory to store all its pointers in the crunch list.	**Mandrake:** http://www.mandrakesecure.net/en/ftp.php **Slackware:** ftp://ftp.slackware.com/pub/slackware/	Sysklogd Crunch_List Remote Denial of Service	Low	Bug discussed in newsgroups and websites.

[25] waraxe-2004-SA#027, May 5, 2004.
[26] Bugtraq, April 26, 2004.
[27] Secunia Advisory, SA11559, May 6, 2004.
[28] Mandrakelinux Security Update Advisory, MDKSA-2004:038, April 29, 2004.
[29] Slackware Security Advisory, SSA:2004-124-02, May 3, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [30]	Windows NT 4.0/2000, 2003, XP, Unix	Web Jetadmin 6.5, 7.0	Multiple vulnerabilities exist: a vulnerability exists when a URL is followed by the period character, which could let a remote malicious user obtain sensitive information; a vulnerability exist in pages that are generated by the '.hts' script, which could let a remote malicious user obtain sensitive information; a vulnerability exists because the encryption method used allows a remote malicious user to monitor encrypted passwords as they are transmitted over the network and then replay them at a later time to obtain unauthorized access; a vulnerability exists when a specially crafted HTTP POST request is submitted, which could let a remote malicious user obtain unauthorized access to internal functions; a vulnerability exists when a remote malicious user submits a specially crafted POST request to write user-controlled data to the 'cache.ini' file, which could lead to the execution of arbitrary code; and a vulnerability exists in the 'ExecuteFile' function, which could let a remote malicious user execute arbitrary programs with root or SYSTEM privileges.	Upgrades available at: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBPI01026	Web Jetadmin Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Root access exploit script has been published.
IBM[31]	Unix	AIX 5.1, 5.2	Multiple vulnerabilities exist: a symlink vulnerability exists in some LVM commands due to the insecure creation of temporary files, which could let a malicious user cause a Denial of Service, or destroy data; and buffer overflow vulnerabilities exist in the 'putlvcb' and 'getlvcb' commands, which could let a malicious user execute arbitrary code.	Updates available at: ftp://aix.software.ibm.com/aix/efixes/security/lvmcmd_efix.tar.Z	Multiple IBM AIX LVM Utilities Symbolic Link & Buffer Overflows	Low/ Medium/ **High** **(Low if a DoS; Medium if data can be corrupt-ed; High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.

[30] HP Security Bulletin HPSBPI01026, April 27, 2004.
[31] IBM Security Advisory, APR-22-2004-LVM, April 22, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[32]	Unix	AIX 5.1, 5.2	Vulnerabilities exist because some console commands use temporary files in an unsafe manner, which could let a malicious user cause a Denial of Service, destroy data, or obtain elevated privileges.	Updates available at: ftp://aix.software.ibm.com/aix/efixes/security/conscmd_efix.tar.Z	AIX Console Command Temporary Files	Low/ Medium (Medium if data can be destroyed or elevated privileges obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
Jelsoft[33]	Multiple	vBulletin 2.0, beta 2&3, 2.0.1, 2.0.2, 2.2.0-2.2.9 can, 2.3, 2.3.3, 2.3.4, 3.0.0 can4, 3.0.0, 3.1.0, 3.2.0, 3.3.0	A vulnerability exists when creating a new forum due to insufficient sanitization of user-supplied input, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	VBulletin Forum Creation HTML Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
JForum[34]	Windows, Unix	Java Web Forum RC1&2, beta, beta2&3	An input validation vulnerability exists which could let a remote malicious user obtain unauthorized access to a restricted forum.	Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=15940	JForum Unauthorized Forum Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
KAME Project[35] ***Apple issues advisory[36]***	**Unix,** ***MacOS X 10.2.8, 10.3.3***	**Racoon** ***Apple Mac OS X 10.2.8, 10.3.3, Mac OS X Server 10.2.8, 10.3.3***	**A Denial of Service vulnerability exits due to an error when allocating memory for ISAKMP messages.**	**Patch available at: http://www.securityfocus.com/data/vulnerabilities/patches/racoon_patch** ***Apple:*** **http://download.info.apple.com/Mac_OS_X/**	**Racoon Malformed ISAKMP Packet Denial of Service**	**Low**	**Bug discussed in newsgroups and websites.**
KAME Project[37]	Unix	Racoon 20040405, 20030711, Racoon	A remote Denial of Service vulnerability exists due to an error when processing certain malformed IKE messages.	Upgrades available at: ftp://ftp.kame.net/pub/kame/snap/kame-20040503-openbsd34-snap.tgz	Racoon Remote IKE Message Denial of Service CVE Name: CAN-2004-0392	Low	Bug discussed in newsgroups and websites.

[32] IBM Security Advisory, APR-22-2004-LVM, April 22, 2004.
[33] SecurityFocus, May 5, 2004.
[34] SecurityTracker Alert, 1009972, April 28, 2004.
[35] Secunia Advisory, SA11410, April 19, 2004.
[36] Apple Security Advisory, APPLE-SA-2004-05-03, May 3, 2004.
[37] SecurityFocus, May 6, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Kine-sphere Corpora-tion[38] ***Upgrade now available*** [39]	**Windows**	**eXchange POP3 4.0, 5.0**	**A buffer overflow vulnerability exists due to a boundary error when handling SMTP connections, which could let a remote malicious user execute arbitrary code.**	***Upgrade available at:*** **http://www.exchangepop3.com/download.html**	**Exchange POP3 Remote Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.**
LCDProc [40] ***Exploit script published*** [41] ***Another exploit published*** [42]	**Unix**	**LCDProc 0.3, 0.4, 0.4.1 -r1, 4.0, 4.1-4.4**	**Multiple vulnerabilities exist: a buffer overflow vulnerability exists, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'parse_all_client_messages()' Function, which could let a remote malicious user execute arbitrary code; and a buffer overflow and format string vulnerability exists in the 'test_func_func()' function, which could let a remote malicious user execute arbitrary code.**	**Upgrade available at:** **http://lcdproc.omnipotent.net/download/lcdproc-0.4.5.tar.gz**	**LCDd Multiple Remote Vulnerabil-ities**	**High**	**Bug discussed in newsgroups and websites.** ***Proof of Concept exploit script has been published.***
McAfee[43]	Windows	Security Installer Control System 4.0 .0.81	A vulnerability exists due to the installation of several non-secure ActiveX controls, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Security Installer Control System ActiveX Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Michael Jennings [44, 45]	Unix	Eterm 0.8.10, 0.9.1	A vulnerability exists in the window title reporting feature, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://www.eterm.org/download/ **Debian:** http://security.debian.org/pool/updates/main/e/eterm **Mandrake:** http://www.mandrakesecure.net/en/ftp.php	ETerm Window Title Reporting Escape Sequence Command Execution CVE Name: CAN-2003-0068	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[38] Bugtraq, April 19, 2004.
[39] SecurityFocus, May 6, 2004.
[40] Priv8 Security Research - #2004-001, April 8, 2004.
[41] PacketStorm, April 9, 2004.
[42] SecurityFocus, April 27, 2004.
[43] SecurityTracker Alert,1009956, April 27, 2004.
[44] Mandrake Linux Security Update Advisory, MDKSA-2003:040, April 1, 2004.
[45] Debian Security Advisory, DSA 496-1, April 29, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [46]	Windows	ASP 3.0, ASP.NET 1.0, 1.1	A vulnerability exists in Microsoft Internet Information Server (IIS) in the processing of certain cookie values by Active Server Pages (ASP) scripts, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ASP.NET Malformed HTTP Request Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft [47]	Windows 95/98/ME/ NT 4.0/2000, XP, 2003	Internet Explorer 5.0, 5.0.1, SP1-SP4, 5.5, SP1&SP2, 6.0, SP1	A remote Denial of Service vulnerability exists when a malicious user creates a malicious site that employs the 'onLoad' event and the 'window.location' javascript method to access a local file.	No workaround or patch available at time of publishing.	Internet Explorer Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft [48]	Windows 98/ME/NT 4.0/2000, XP, 2003	Internet Explorer 6.0, SP1	A vulnerability exists because it is possible to embed a certificate and content from a foreign domain via SSL into a web page, which could let a remote malicious user employ another site's certificate to cause the target user's browser to appear to be connected to the other site. *Note: While the connection will appear to be secure, as denoted by the closed lock icon in the right bottom corner of the browser window, the spoofed certificate may not be manually inspected (by clicking the lock icon).*	No workaround or patch available at time of publishing.	Internet Explorer SSL Icon Error	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[46] AppSecInc Security Alert, May 5, 2004.
[47] SecurityFocus, May 11, 2004.
[48] Bugtraq, April 30, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63] *Avaya releases an advisory to announce Avaya System Products shipping on Microsoft platforms are also affected by this vulnera-bility*[64] *More exploits published* [65]	Windows 98/SE/ME, NT 4.0/2000, XP, 2003	Windows NT Work-station 4.0 SP6a, NT Server 4.0 SP6a, 4.0, Terminal Server Edition SP6, Windows 2000, SP2-SP4, XP, SP1, XP 64-Bit Edition, SP1, 64-Bit Edition Version 2003, Windows Server™ 2003, 2003 64-Bit Edition, Net-Meeting, Windows 98, SE, ME; *Avaya Definity One Media Servers, IP600 Media Servers, S3400 Modular Messag-ing, S8100 Media Servers*	A vulnerability exists in LSASS, which could let a remote malicious user execute arbitrary code; a DoS vulnerability exists in LSASS when processing LDAP requests; a vulnerability exists in the PCT protocol, which could let a remote malicious user execute arbitrary code; a vulnerability exists in Winlogon, which could let a remote malicious user execute arbitrary code; a vulnerability exists when rendering Metafiles, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'Help and Support Center' when handling HCP URLs, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the Utility Manager, which could let a remote malicious user obtain SYSTEM privileges; a vulnerability exists in Windows task management, which could let a remote malicious user execute arbitrary code; a vulnerability exists when creating entries in the Local Descriptor Table, which could let a malicious user obtain elevated privileges; a vulnerability exists in the H.323 protocol, which could let a malicious user execute arbitrary code; a vulnerability e xists in the Virtual DOS Machine subsystem, which could let a malicious user obtain elevated privileges; a DoS vulnerability exists in Negotiate Security Software Provider, which could also let a remote malicious user execute arbitrary code; a DoS vulnerability exists in the SSL library & ASN.1 Library, which could also let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx *Avaya advise that customers follow the Microsoft recommendations for the resolution of this issue.*	Microsoft Windows Multiple Vulnerabil-ities CVE Names: CAN-2003-0533, CAN-2003-0663, CAN-2003-0719, CAN-2003-0806, CAN-2003-0906, CAN-2003-0907, CAN-2003-0908, CAN-2003-0909, CAN-2003-0910, CAN-2003-0117, CAN-2003-0118, CAN-2003-0119, CAN-2004-0120, CAN-2004-0123	Low/ Medium/ High (Low if a DoS; Medium if elevated privileges obtained; and High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. *Exploit script has been published for the PCT protocol vulnerably.* *More exploit scripts have been published. A White paper has been also published that analyzes the SSL PCT vulnerability and gives full details on how exploitation has been performed and what it takes for working exploits to be created.*

[49] Microsoft Security Bulletin, MS04-011, April 13, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mister[66] **_Upgrade now available_**[67]	**Windows, Unix**	**Protector System 1.15 b1**	**Multiple vulnerabilities exist: a vulnerability exists in the 'blocker_query.php' script when an invalid value is supplied to the 'portNum' parameter, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the 'blocker_query.php' script due to insufficient verification of the 'target' and portNum' parameters, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists due to insufficient of input passed to 'GET' queries, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability exists because it is possible to bypass the SQL injection filter system, which could let a remote malicious user bypass anti-sql-injection filters.**	**_Upgrade available at:_ http://protector.warcenter.se/modules.php?name=Downloads&d_op=viewdownloaddetails&lid=17&title=Fix%202%20Blocker**	**Multiple Protector System Multiple Vulnerabilities**	**Medium/ High (High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.**
moodle.org [68]	Windows, Unix	moodle 1.1.1, 1.2, 1.2.1	A Cross-Site Scripting vulnerability exists in 'help.php' due to insufficient sanitization of the 'text' parameter, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrades available at: http://moodle.org/download.php/moodle/moodle-latest.tgz	Moodle Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[50] VU#260588, http://www.kb.cert.org/vuls/id/260588.
[51] VU#150236, http://www.kb.cert.org/vuls/id/150236.
[52] VU#255924, http://www.kb.cert.org/vuls/id/255924.
[53] VU#638548, http://www.kb.cert.org/vuls/id/638548.
[54] VU#783748, http://www.kb.cert.org/vuls/id/783748.
[55] VU#353956, http://www.kb.cert.org/vuls/id/353956.
[56] VU#122076, http://www.kb.cert.org/vuls/id/122076.
[57] VU#206468, http://www.kb.cert.org/vuls/id/206468.
[58] VU#526084, http://www.kb.cert.org/vuls/id/526084.
[59] VU#547028, http://www.kb.cert.org/vuls/id/547028.
[60] VU#639428, http://www.kb.cert.org/vuls/id/639428.
[61] VU#471260, http://www.kb.cert.org/vuls/id/471260.
[62] VU#753212, http://www.kb.cert.org/vuls/id/753212.
[63] VU#586540, http://www.kb.cert.org/vuls/id/586540.
[64] SecurityFocus, April 21, 2004.
[65] Packet storm, May 4, 2004
[66] Securiteam, April 25, 2004.
[67] SecurityFocus, April 27, 2004.
[68] Securiteam, May 4, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[69]	Windows	Microsoft Outlook Express 6.0; Qual-comm Eudora 6.0 .22, 6.0, 6.0.1, 6.0.3, 6.1	A vulnerability exists due to a failure to properly display the URL in the status bar if a specially crafted long URL containing multiple spaces, which could let a malicious user hide spoofed URLs.	No workaround or patch available at time of publishing.	Eudora Embedded Hyperlink URI Obfuscation Weakness	Medium	Bug discussed in newsgroups and websites. It is reported that this issue is being actively exploited in the wild by an e-mail that is being spammed to end-users.
Multiple Vendors[70]	Windows, Unix	Copper-mine Photo Gallery 1.0 RC3, 1.1 beta 2, 1.1 .0, 1.2, 1.2.1, 1.2.2 b; Francisco Burzi PHP-Nuke 6.9, 7.0, FINAL, 7.1, 7.2	Multiple vulnerabilities exist: an input validation vulnerability exists if error messages hasn't been turned off in PHP, which could let a remote malicious user obtain sensitive information; an input validation vulnerability exists in the 'menu.inc.php' script due to insufficient verification of the 'CPG_URL' parameter, which could let a remote malicious user execute arbitrary HTML or script code; and an input validation vulnerability exists due to a failure to verify certain parameters before using them to include files, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Photo Gallery Multiple Input Validation Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required; however, Proof of Concepts exploits have been published.
Multiple Vendors[71]	Unix	Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; GNU Emacs 20.0-20.6, 21.2	A vulnerability exists in the Emacs film library due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges.	**Debian:** http://security.debian.org/pool/updates/main/f/flim/	Emacs film Library Insecure Temporary File Creation CVE Name: CAN-2004-0422	Medium	Bug discussed in newsgroups and websites.

[69] SecurityFocus, May 7, 2004.
[70] waraxe-2004-SA#026, May 2, 2004.
[71] Debian Security Advisory, DSA 500-1, May 2, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[72]	Unix	Kolab Groupware Server 1.0, 1.0.1, 1.0.3, 1.0.5, 1.0.6, 1.0.7, 1.0.8 OpenPKG OpenPKG 2.0	A vulnerability exists because passwords are stored in plaintext format, which could let a malicious user obtain sensitive information. .	Upgrades available at: http://www.erfrakon.de/projects/kolab/download/ **OpenPKG:** ftp://ftp.openpkg.org/release/2.0/UPD/kolab-20040217-2.0.2.src.rpm	Groupware Server OpenLDAP Plaintext Password Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors[73] ***More vendor advisories issued[74,75, 76, 77, 78]***	**Unix**	**Linux kernel 2.4.22, 2.4.23, 2.4.23 -ow2, 2.4.23 -pre9, 2.4.24, 2.4.24 -ow1, 2.4.25, 2.6.1, rc1&4c2, 2.6.2, 2.6.3**	**An integer overflow vulnerability exists in the 'ip_setsockopt()' function when handling the 'MCAST_MSFILTER' socket option, which could let a malicious user cause a Denial or Service or execute arbitrary code.**	**Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.26.tar.bz2 RedHat: http://rhn.redhat.com/errata/RHSA-2004-183.html *Engarde:* http://infocenter.guardiandigital.com/advisories/ *Fedora:* http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ *Mandrake:* http://www.mandrakesecure.net/en/advisories/ *Slackware:* ftp://ftp.slackware.com/pub/slackware/ *SuSE:* ftp://ftp.suse.com/pub/suse/**	**Linux Kernel MCAST_ MSFILTER Integer Overflow CVE Name: CAN-2004-0424**	**Low/High (High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Proof of Concept Denial of Service exploit script has been published.**
Multiple Vendors[79] ***SuSE issues advisory[80]***	**Unix**	**Linux kernel 2.5.0-2.5.69, 2.6, 2.6 -test1-test11, 2.6.1, rc1&rc2, 2.6.2-2.6.5**	**A vulnerability exists in the 'cpufreq_userspace' proc handler, which could let a malicious user obtain sensitive information.**	**Update available at: http://www.kernel.org/pub/linux/kernel/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ SuSE:** ftp://ftp.suse.com/pub/suse/x86_64/update/	**Linux Kernel CPUFreq Proc Handler Information Disclosure CVE Name: CAN-2004-0228**	**Medium**	**Bug discussed in newsgroups and websites.**

[72] OpenPKG Security Advisory, OpenPKG-SA-2004.019, May 5, 2004.
[73] RedHat Security Advisory, RHSA-2004:183-03, April 22, 2004.
[74] Fedora Update Notification, FEDORA-2004-111, April 22, 2004.
[75] Mandrakelinux Security Update Advisory, MDKSA-2004:037, April 27, 2004.
[76] Guardian Digital Security Advisory, ESA-20040428-004, April 28, 2004
[77] Slackware Security Advisory, SSA:2004-119-01, April 29, 2004.
[78] SUSE Security Announcement, SuSE-SA:2004:010, May 5, 2004.
[79] Fedora Update Notification, FEDORA-2004-111, April 22, 2004.
[80] SUSE Security Announcement, SuSE-SA:2004:010, May 5, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[81]	Unix	Linux kernel 2.6-2.6.5	A vulnerability exists because the 'exit_thread()' function does not invalidate per-TSS IO bitmap pointers before certain processes exit, which could let a malicious user cause a Denial of Service or obtain elevated privileges.	No workaround or patch available at time of publishing.	Linux Kernel Local IO Access Inheritance	Low/ Medium (Medium if elevated privileges can be obtained)	Bug discussed in newsgroups and websites.
Multiple Vendors[82, 83]	Unix	MPlayer 1.0 pre3try2; xine-lib 1-rc3a-rc3c, 1-rc2, 1-beta1-beta11	Several buffer overflow vulnerabilities exist in 'realrtsp' code shared between MPlayer and xine-lib, which could let a remote malicious user execute arbitrary code.	**Mplayer:** http://mplayer.dev.hu/homepage/design6/dload.html **Slackware:** ftp://ftp.slackware.com/pub/slackware/ **Xine:** http://xinehq.de/index.php/releases	MPlayer/ Xine-Lib Multiple RealRTSP Buffer Overflows	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[84, 85]	Unix	Linux kernel 2.4.0-test1-test12, 2.4-2.4.25	A buffer overflow vulnerability exists in the 'panic()' function call, which could let a malicious user obtain sensitive information.	**Slackware:** ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/ **SuSE:** ftp://ftp.suse.com/pub/suse/i386/update/	Linux Kernel Panic Function Call Buffer Overflow CVE Name: CAN-2004-0394	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors [86, 87] *Apple issues advisory*[88]	**Unix** *MacOS X 10.2.8, 10.3.3*	**IPsec-Tools, 0.1, 0.2-0.2.4, 0.3, rc1-rc4; KAME Racoon, 20030711** *Apple Mac OS X 10.2.8, 10.3.3, Mac OS X Server 10.2.8, 10.3.3*	**A vulnerability exists due to an error within the 'eay_rsa_verify()' function in 'crypto_openssl.c' which may allow remote malicious holders of valid X.509 certificates to make unauthorized connections to the VPN without being required to be in possession of the corresponding private key.**	**Upgrades available at: http://sourceforge.net/project/showfiles.php?group_id=74601&release_id=228873 Mandrake: http://www.mandrakesecure.net/en/ftp.php** ***Apple:*** **http://download.info.apple.com/Mac_OS_X/**	**Racoon IKE Daemon Unauthorized X.509 Certificate Connection CVE Name: CAN-2004-0155**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.**

[81] Secunia Advisory, SA11577, May 10, 2004.
[82] Xine Security Advisory, XSA-2004-3, April 30, 2004.
[83] Slackware Security Advisory, SSA:2004-124-03, May 3, 2004.
[84] Slackware Security Advisory, SSA:2004-119-01, April 29, 2004.
[85] SUSE Security Announcement, SuSE-SA:2004:010, May 5, 2004.
[86] Mandrakelinux Security Update Advisory, MDKSA-2004:027, April 8, 2004.
[87] VU#552398, https://www.kb.cert.org/vuls/id/552398.
[88] Apple Security Advisory, APPLE-SA-2004-05-03, May 3, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [89, 90, 91, 92, 93] ***More advisories issued*** [94, 95, 96] ***More information released*** [97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108]	**Unix**	**Gaim version 0.75 & prior**	**Multiple buffer overflow vulnerabilities exist due to boundary errors in the YMSG protocol handler, the oscar protocol handler, various utility functions, and the HTTP proxy connection handling, which could let a remote malicious user execute arbitrary code.**	**Upgrade available at:** http://prdownloads.sourceforge.net/ultramagnetic/ultramagnetic-0.81.tar.bz2?download **Debian:** http://security.debian.org/pool/updates/main/g/gaim/ **Mandrake:** http://www.mandrakesecure.net/en/advisories/ **RedHat:** ftp://updates.redhat.com/ **Slackware:** ftp://ftp.slackware.com/pub/slackware/ **SuSE:** ftp://ftp.suse.com/pub/suse/i386/update/ ***Conectiva:*** ftp://atualizacoes.conectiva.com.br/ ***Fedora:*** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ ***SGI:*** ftp://patches.sgi.com/support/free/security/patches/ProPack/2.3/	**Gaim Multiple Remote Buffer Overflow Vulnerabilities** **CVE Names: CAN-2004-0005, CAN-2004-0006, CAN-2004-0007. CAN-2004-0008**	**High**	**Bug discussed in newsgroups and websites.**

[89] Red Hat Security Advisory, RHSA-2004:032-01, January 26, 2004.
[90] Slackware Security Advisory, SSA:2004-026-01, January 27, 2004.
[91] SuSE Security Announcement, SuSE-SA:2004:004, January 29, 2004.
[92] Mandrake Linux Security Update Advisory, MDKSA-2004:006-1, January 30, 2004
[93] Debian Security Advisory, DSA 434-1, February 5, 2004.
[94] Conectiva Linux Security Announcement, CLA-2004:813, February 10, 2004.
[95] SGI Security Advisory, 20040201-01-U, February 11, 1004.
[96] Fedora Update Notification, FEDORA-2004-070, February 16, 2004.
[97] VU#197142, http://www.kb.cert.org/vuls/id/197142.
[98] VU#779614, http://www.kb.cert.org/vuls/id/779614.
[99] VU#444158, http://www.kb.cert.org/vuls/id/444158.
[100] VU#871838, http://www.kb.cert.org/vuls/id/871838.
[101] VU#527142, http://www.kb.cert.org/vuls/id/527142.
[102] VU#297198, http://www.kb.cert.org/vuls/id/297198.
[103] VU#371382, http://www.kb.cert.org/vuls/id/371382.
[104] VU#503030, http://www.kb.cert.org/vuls/id/503030.
[105] VU#190366, http://www.kb.cert.org/vuls/id/190366.
[106] VU#226974, http://www.kb.cert.org/vuls/id/226974.
[107] VU#655974, http://www.kb.cert.org/vuls/id/655974.
[108] VU#404470, http://www.kb.cert.org/vuls/id/404470.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [109, 110]	Unix	Mr. S.K. LHA 1.14, 1.15, 1.17; RARLAB WinRar 3.20; RedHat lha-1.14i-9.i386.rpm; WinZip 9.0	Multiple vulnerabilities exist: two buffer overflow vulnerabilities exist when creating a carefully crafted LHA archive, which could let a remote malicious user execute arbitrary code; and several Directory Traversal vulnerabilities exist, which could let a remote malicious user corrupt/overwrite files in the context of the user who is running the affected LHA utility.	**RedHat:** ftp://up dates.redhat.com/9/en/os/i386/lha-1.14i-9.1.i386.rpm **Slackware:** ftp://ftp.slackware.com/pub/slackware/	Multiple LHA Buffer Overflow/ Directory Traversal Vulnerabilities CVE Names: CAN-2004-0234, CAN-2004-0235	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Multiple Vendors [111, 112, 113]	Unix	Linux kernel 2.4, 2.4 .0-test1-test12, 2.4.1-2.4.26, 2.6, 2.6 -test1-test12, 2.6.1, rc1&rc2, 2.6.2-2.6.5	A vulnerability exists because memory is allocated for child processes but never freed, which could let a malicious user obtain sensitive information.	**Engarde:** http://infocenter.guardiandigital.com/advisories/ **Fedora:** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/ **Mandrake:** http://www.mandrakesecure.net/en/advisories/	Linux kernel do_fork() Memory Leakage CVE Name: CAN-2004-0427	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors [114, 115] ***More advisories issued*** [116] [117, 118]	**Unix**	**Linux kernel 2.4, 2.4 .0-test1-test12, 2.4.1-2.4.25, 2.6, test1-test11, 2.6.1 -rc1&rc2, 2.6.2-2.6.4**	**A vulnerability exists in the Linux kernel when writing to the XFS file system, which could let a malicious user obtain sensitive information.**	**Upgrade available at: http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.26.tar.bz2 Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/** ***Engarde:*** **http://infocenter.guardiandigital.com/advisories/** ***Fedora:*** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/** ***SGI:*** ***ftp://patches.sgi.com/support/free/security/advisories/***	**Linux Kernel XFS File System Information Leakage CVE Name: CAN-2004-0133**	**Medium**	**Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.**

[109] Red Hat Security Advisory, RHSA-2004:179-01, April 30, 2004.
[110] Slackware Security Advisory, SSA:2004-125-01, May 5, 2004.
[111] Fedora Update Notification, FEDORA-2004-111, April 22, 2004.
[112] Mandrakelinux Security Update Advisory, MDKSA-2004:037, April 27, 2004.
[113] Guardian Digital Security Advisory, ESA-20040428-004, April 28, 2004.
[114] Mandrakelinux Security Update Advisory, MDKSA-2004:029, April 14, 2004.
[115] Trustix Secure Linux Security Advisory, TSLSA-2004-0020, April 15, 2004.
[116] Fedora Update Notification, FEDORA-2004-111, April 22, 2004.
[117] SGI Security Advisory, 20040405-01-U, April 27, 2004.
[118] Guardian Digital Security Advisory, ESA-20040428-004, April 28, 2004

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [119, 120, 121] ***More advisories issued*** [122, 123]	**Unix**	**Linux kernel 2.4, 2.4 .0-test1-test12, 2.4.1-2.4.25, 2.6, test1-test11, 2.6.1 -rc1&rc2, 2.6.2-2.6.4**	**Multiple vulnerabilities exist: a vulnerability exists due to information leaks within the JFS file system code, which could let a malicious user obtain sensitive information; and a Denial of Service vulnerability exists in the Linux Sound Blaster driver.**	**Upgrade available at:** http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.26.tar.bz2 **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **SuSE:** ftp://ftp.suse.com/pub/suse/i386/update/ **Trustix:** http://http.trustix.org/pub/trustix/updates/ ***Engarde:*** http://infocenter.guardiandigital.com/advisories/ ***Fedora:*** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/	**Linux Kernel Multiple Vulnerabilities** **CVE Names: CAN-2004-0178, CAN-2004-0181**	**Low/ Medium** **(Medium if sensitive information can be obtained)**	**Bug discussed in newsgroups and websites.**
Multiple Vendors [124, 125, 126] ***Another exploit published*** [127]	**Multiple**	**Multiple (See advisory located at: http://www.uniras.gov.uk/vuls/2004/236929/index.htm for complete list)**	**A vulnerability exists that affects implementations of the Transmission Control Protocol (TCP) that comply with the Internet Engineering Task Force's (IETF's) Requests For Comments (RFCs) for TCP. The impact of this vulnerability varies by vendor and application but could let a remote malicious user cause a Denial of Service, or allow unauthorized malicious users to inject malicious data into TCP streams.**	**List of updates available at:** http://www.uniras.gov.uk/vuls/2004/236929/index.htm	**Multiple Vendor TCP Sequence Number Approximation** **CVE Name: CAN-2004-0230**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.** **Vulnerability has appeared in the press and other public media.**
Multiple Vendors [128, 129, 130]	Unix	ProFTPD Project ProFTPD 1.2.9; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	A vulnerability exists because a CIDR based ACL entry will act as an 'AllowAll' directive, which could let a malicious user bypass access control rules.	**Mandrake:** http://www.mandrakesecure.net/en/ftp.php **OpenPKG:** ftp://ftp.openpkg.org/ **Trustix:** http://www.trustix.org/errata/misc/2004/TSL-2004-0025-multi.asc.txt	ProFTPD CIDR Access Control Rule Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[119] Mandrakelinux Security Update Advisory, MDKSA-2004:029, April 14, 2004.
[120] SUSE Security Announcement, SuSE-SA:2004:009, April 14, 2004.
[121] Trustix Secure Linux Security Advisory, TSLSA-2004-0020, April 15, 2004.
[122] Fedora Update Notification, FEDORA-2004-111, April 22, 2004.
[123] Guardian Digital Security Advisory, ESA-20040428-004, April 28, 2004
[124] NISCC Vulnerability Advisory, 236929, April 23, 2004.
[125] VU#415294, http://www.kb.cert.org/vuls/id/415294.
[126] TA04-111A, http://www.us-cert.gov/cas/techalerts/TA04-111A.html.
[127] SecurityFocus, May 11, 2004.
[128] Mandrakelinux Security Update Advisory, MDKSA-2004:041, April 30, 2004.
[129] OpenPKG Security Advisory, OpenPKG-SA-2004.018, April 30, 2004.
[130] Trustix Secure Linux Security Advisory, TSLSA-2004-0025, April 30, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [131, 132, 133] ***RedHat issues advisory*** [134]	**Unix**	**Slackware Linux – current, 9.1; utempter utempter 0.5.2, 0.5.3**	**Multiple vulnerabilities exist: a vulnerability exists due to an input validation error that causes the application to exit improperly, which could let a malicious user obtain root privileges; and a vulnerability exists due to a failure to validate buffer boundaries, which could let a malicious user cause a Denial of Service.**	**Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **Slackware:** **ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/l/utempter-1.1.1-i486-1.tgz** ***RedHat:*** **ftp://updates.redhat.com/9/en/os/SRPMS/utempter-0.5.5-2.RHL9.0.src.rpm**	**UTempter Multiple Local Vulnerabilities** **CVE Name: CAN-2004-0233**	**Low/High** **(High if root access can be obtained)**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**
Multiple Vendors [135, 136, 137, 138]	Unix	Debian Linux 3.0, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; rsync 2.3.1, 2.3.2 -1.3, 2.3.2 -1.2, sparc, PPC, m68k, intel, ARM, alpha, 2.3.2, 2.4.0, 2.4.1, 2.4.3-2.4.6, 2.4.8, 2.5.0-2.5.7, 2.6	A vulnerability exists due to insufficient sanitization of user-supplied path values, which could let a remote malicious user modify system information or obtain unauthorized access.	**Debian:** http://security.debian.org/pool/updates/main/r/rsync **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **Rsync:** http://rsync.samba.org/ftp/rsync/rsync-2.6.1.tar.gz **Slackware:** ftp://ftp.slackware.com/pub/slackware/ **Trustix:** http://www.trustix.org/errata/misc/2004/TSL-2004-0024-rsync.asc.txt	RSync Path Validation CVE Name: CAN-2004-0426	Medium	Bug discussed in newsgroups and websites.

[131] Slackware Security Advisory, SSA:2004-110-01, April 19, 2004.
[132] Fedora Update Notification, FEDORA-2004-108, April 21, 2004.
[133] Mandrakelinux Security Update Advisory, MDKSA-2004:031-1, April 21, 2004.
[134] Red Hat Security Advisory, RHSA-2004:175-01, April 30, 2004.
[135] Trustix Secure Linux Security Advisory, 2004-0024, April 30, 2004.
[136] Debian Security Advisory, DSA 499-1, May 2, 2004.
[137] Slackware Security Advisory, SSA:2004-124-01, May 3, 2004.
[138] Mandrakelinux Security Update Advisory, MDKSA-2004:042, May 11, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [139, 140, 141, 142]	Unix	Gentoo Linux 0.5, 0.7, 1.1 a, 1.2, 1.4_rc1-3, 1.4; Midnight Com-mander 4.5.40-4.5.55, 4.6; SGI ProPack 2.3, 2.4	Multiple vulnerabilities exist including several buffer overflows, a format string vulnerability, and a temporary file and directory creation vulnerability, which could let a malicious user obtain unauthorized access, cause a Denial of Service, or execute arbitrary code..	**Debian:** http://security.debian.org/pool/updates/main/m/mc **Fedora:** http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1 **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **RedHat:** ftp://updates.redhat.com/9/en/os/i386/mc-4.6.0-14.9.i386.rpm	Midnight Commander Multiple Unspecified Vulnerabilities CVE Names: CAN-2004-0226, CAN-2004-0231, CAN-2004-0232	Low/ Medium/ **High** **(Low if a DoS; Medium is unauth-orized access can be obtained; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Multiple Vendors [143, 144, 145, 146, 147] ***More advisories issued*** [148, 149]	**Unix**	**Linux kernel 2.4, 2.4 .0-test1-test12, 2.4.1-2.4.25**	**A buffer overflow vulnerability exists due to a boundary error within the ISO9660 ('isofs') file system component when handling symbolic links, which could let a malicious user execute arbitrary code.**	**Upgrade available at:** **http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.26.tar.bz2** **Debian:** **http://security.debian.org/pool/updates/main/k/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **RedHat:** **ftp://updates.redhat.com/9/en/os/** **SuSE:** **ftp://ftp.suse.com/pub/suse/i386/update/** **Trustix:** **http://http.trustix.org/pub/trustix/updates/** ***Engarde:*** **http://infocenter.guardiandigital.com/advisories/** ***SGI:*** ***ftp://patches.sgi.com/support/free/security/advisories/***	**Linux Kernel ISO9660 File System Buffer Overflow** **CVE Name: CAN-2004-0109**	**High**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**

[139] Debian Security Advisory, DSA 497-1, April 29, 2004.
[140] Fedora Update Notification, FEDORA-2004-112, April 30, 2004.
[141] Mandrakelinux Security Update Advisory, MDKSA-2004:039, April 30, 2004.
[142] Red Hat Security Advisory, RHSA-2004:173-01, April 30, 2004.
[143] Debian Security Advisories, DSA 479-1, 479-2, DSA 482-1, & DSA 491-1, April 14 & 17, 2004.
[144] Mandrakelinux Security Update Advisory, MDKSA-2004:029, April 14, 2004.
[145] SUSE Security Announcement, SuSE-SA:2004:009, April 14, 2004.
[146] Trustix Secure Linux Security Advisory, TSLSA-2004-0020, April 15, 2004.
[147] Red Hat Security Advisory, RHSA-2004:166-01, April 21, 2004.
[148] SGI Security Advisory, 20040405-01-U, April 27, 2004.
[149] Guardian Digital Security Advisory, ESA-20040428-004, April 28, 2004

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [150, 151, 152, 153, 154] ***Engarde issues advisory*** [155]	**Unix**	**Linux kernel 2.4, 2.4 .0-test1-test12, 2.4.1-2.4.25, 2.6, test1-test11, 2.6.1 -rc1&rc2, 2.6.2-2.6.4**	**A vulnerability exists in the Linux kernel when writing to an ext3 file system due to a design error that causes some kernel information to be leaked, which could let a malicious user obtain sensitive information.**	**Upgrade available at:** http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.26.tar.bz2 **Conectiva:** ftp://ul.conectiva.com.br/updates/1.0/ **Debian:** http://security.debian.org/pool/updates/main/k/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **RedHat:** ftp://updates.redhat.com **Trustix:** http://http.trustix.org/pub/trustix/updates/ ***Engarde:*** http://infocenter.guardiandigital.com/advisories/	**Linux Kernel EXT3 File System Information Leakage** **CVE Name: CAN-2004-0177**	**Medium**	**Bug discussed in newsgroups and websites. Vulnerability may be exploited via a web browser.**

[150] Mandrakelinux Security Update Advisory, MDKSA-2004:029, April 14, 2004.
[151] Trustix Secure Linux Security Advisory, TSLSA-2004-0020, April 15, 2004.
[152] Debian Security Advisories, DSA 489-1 & 491-1, April 17, 2004.
[153] Conectiva Security Advisory, CLSA-2004:829, April 15, 2004.
[154] Red Hat Security Advisories, RHSA-2004:166-01 & 166-08, April 21, 2004.
[155] Guardian Digital Security Advisory, ESA-20040428-004, April 28, 2004

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [156, 157, 158, 159, 160, 161]	Unix	libpng 1.0, 1.0.5-1.0.14, libpng3 1.2 .0-1.2.5; OpenPKG 1.3, 2.0; RedHat libpng-1.2.2-16.i386.rpm, libpng-1.2.2-20.i386.rpm, libpng-devel-1.2.2-20.i386.rpm, ibpng10-1.0.13-11.i386.rpm, libpng10-1.0.13-8.i386.rpm, libpng10-devel-1.0.13-11.i386.rpm, libpng10-devel-1.0.13-8.i386.rpm; Trustix Secure Enterprise Linux 2.0, Secure Linux 2.0, 2.1	A remote Denial of Service vulnerability exists when handling certain types of malformed PNG images.	**Debian:** http://security.debian.org/pool/updates/main/libp/libpng/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **OpenPKG:** ftp://ftp.openpkg.org/release/ **RedHat:** ftp://updates.redhat.com/9/en/os/i386/ **Slackware:** ftp://ftp.slackware.com/pub/slackware/ **Trustix:** http://www.trustix.org/errata/misc/2004/TSL-2004-0025-multi.asc.txt	LibPNG PNG Image Remote Denial of Service CVE Name: CAN-2004-0421	Low	Bug discussed in newsgroups and websites.

[156] Debian Security Advisory, DSA 498-1, April 30, 2004.
[157] Mandrakelinux Security Update Advisory, MDKSA-2004:040, April 30, 2004.
[158] OpenPKG Security Advisory, OpenPKG-SA-2004.017, April 30, 2004.
[159] Red Hat Security Advisory, RHSA-2004:181-01, April 30, 2004.
[160] Trustix Secure Linux Security Advisory, TSLSA-2004-0025, April 30, 2004.
[161] Slackware Security Advisory, SSA:2004-124-04, May 3, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NetWin[162]	Windows NT 4.0/2000, 2003, XP	Surge LDAP 1.0g, 1.0f, 1.0 e, 1.0d, 1.0b, 1.0 a	A vulnerability exists due to an authentication error within the administrative web interface, which could let a remote malicious user bypass authentication and obtain administrative access.	No workaround or patch available at time of publishing.	SurgeLDAP Web Administration Authentication Bypass	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Novell[163]	Windows NT 4.0/2000, 2003	eDirectory 8.7	A vulnerability exists in the Role Based Services (RBS) component because trustee assignments allocated to the ROOT object may be higher than the minimum required to complete a particular task, which could let a malicious user obtain administrative privileges.	**Workaround:** Novell suggests that the following steps be taken to limit the exposure to this issue: • Modify the rights assignment for the Role AND/OR • Make the Role trustee assignment at the Resource to be managed, change the scope.	eDirectory RBT Insecure Role Permissions	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
OMail[164]	Unix	OMail webmail 0.97.3, 0.98.3, 0.98.5	A vulnerability exists due to insufficient sanitization of shell metacharactes that are passed through URI parameters, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	OMail Webmail Remote Command Execution Variant	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[162] SecurityFocus, May 6, 2004.
[163] Novell Technical Information Document, TID10092504, April 27, 2004.
[164] SecurityFocus, May 4, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
OpenBB [165]	Windows, Unix	OpenBB 1.0 .0 beta1, RC1-RC3, 1.0.5, 1.0.6	Multiple vulnerabilities exist: A Cross-Site Scripting vulnerability exists due to insufficient verification of input passed to certain parameters in various scripts, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists due to insufficient verification of input passed to certain parameters in various before it is used in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability exists because multiple administrative, moderator, and user functions are accessible through GET requests, which could let a remote malicious execute arbitrary commands; a vulnerability exists in the 'myhome.php' script, which could le a remote malicious user obtain sensitive information; and a vulnerability exists due to insufficient verification of uploaded avatars, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	OpenBB Multiple Input Validation Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required; however, Proofs of Concept exploits have been published.
OpenRDF .org[166]	Windows, Unix	Sesame RDF container 1.0, PRE-1 - PRE4	A vulnerability exists in 'SesameServlet.setSession Context()' due to a failure to properly secure repository contents, which could let a remote malicious user obtain sensitive information.	Upgrades available at: http://heanet.dl.sourceforge.net/sourceforge/sesame/sesame-1.0.1-bin.tar.gz	Sesame Unauthorized Repository Access	Medium	Bug discussed in newsgroups and websites.

[165] GulfTech Security Research Team Advisory, April 25, 2004.
[166] SecurityFocus, April 30, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Peter Zelezny [167, 168] ***More advisories issued and exploit script published*** [169, 170, 171]	**Unix**	**X-Chat 1.8-1.8.2, 1.8.6-1.8.9, 2.0.1, 2.0.5-2.0.8**	**A buffer overflow vulnerability exists in the SOCKS 5 proxy code, which could let a remote malicious user execute arbitrary code.**	**Patch available at:** **http://www.xchat.org/files/source/2.0/patches/xc208-fixsocks5.diff** **Debian:** **http://security.debian.org/pool/updates/main/x/xchat/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** ***Netwosix:*** **http://www.netwosix.org/adv14.html** ***RedHat:*** **ftp://updates.redhat.com/9/en/os/**	**XChat SOCKS 5 Remote Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
PHP Arena[172]	Unix	PAFileDB 3.0, Beta 3.1	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists in 'pafiledb.php' due to insufficient sanitization of the 'id' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists if error messages hasn't been turned off in PHP because various scripts will return error messages if invalid input is supplied, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PAFileDB Cross-Site Scripting & Information Disclosure	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
PhpwsBB/ phpws-Contacts [173]	Windows, Unix	phpwsbb 0.8, 0.8.1, 0.9.1; phpws Contacts 0.8, 0.8.1, 0.8.2	A vulnerability exists in phpwsbb because it is possible to view message labels (even if anonymous viewing has been turned off) and a vulnerability exists in phpwsContacts in the 'allow_anon_view' setting, which could let a remote malicious user obtain sensitive information.	**Phpwsbb:** http://prdownloads.sourceforge.net/phpwsbb/phpwsbb-0.9.2.tar.gz?download **phpwsContacts:** http://prdownloads.sourceforge.net/phpwscontacts/phpwscontacts-0.8.3.tar.gz?download	PhpwsBB/ phpwsContacts Modules Information Disclosure	Medium	Bug discussed in newsgroups and websites.

[167] Debian Security Advisory, DSA 493-1, April 21, 2004.
[168] Mandrakelinux Security Update Advisory, MDKSA-2004:036, April 22, 2004.
[169] Red Hat Security Advisory, RHSA-2004:177-01, April 30, 2004.
[170] Netwosix Linux Security Advisory, LNSA-#2004-0014, May 1, 2004.
[171] Packet storm, May 4, 2004.
[172] SecurityTracker Alert, 1009966, April 28, 2004.
[173] Secunia Advisory, SA11480, April 26, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
phpx.org [174]	Windows, Unix	PHPX 3.0-3.0.7, 3.1.0-3.1.4, 3.2.0-3.2.6	Multiple vulnerabilities exist: a vulnerability exists in the 'forums.php' script if error messages hasn't been turned off, which could let a remote malicious user obtain sensitive information; a Cross-Site Scripting vulnerability exists due to insufficient verification of input passed to certain parameters in various scripts, which could let a remote malicious user execute arbitrary HTML or script code; and a vulnerability exists due to insufficient sanitization of links to images in private messages, which could let a remote malicious user execute administrative functions.	Upgrades available at: https://sourceforge.net/project/showfiles.php?group_id=67670&package_id=65973&release_id=235919	PHPX Multiple Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, Proofs of Concepts exploit scripts have been published.
phpx.org [175]	Windows, Unix	PHPX 3.0-3.0.7, 3.1.0-3.1.4, 3.2.0-3.2.6	Multiple administrator command execution vulnerabilities exist due to a failure of the application to properly validate access to administrative commands, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrades available at: https://sourceforge.net/project/showfiles.php?group_id=67670&package_id=65973&release_id=235919	PHPX Multiple Administrator Command Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, Proofs of Concepts have been published.
PROPS [176]	Windows, Unix	PROPS 0.6.1	Several vulnerabilities exist: a vulnerability exists in the 'glossary_init()' function in 'lib/glossary.php' due to insufficient validation of user-supplied input in the '$module' and '$format' variables, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists in the 'do_search()' function in 'archives/lib/do_search.php' due to insufficient filtering of HTML code from user-supplied input in the '$search_string' variable, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=29581&package_id=21534&release_id=234433	PROPS Information Disclosure & Cross-Site Scripting	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.

[174] Bugtraq, May 4, 2004.
[175] Bugtraq, May 4, 2004.
[176] Bugtraq, May 1, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Qual-comm[177]	Windows	Eudora 5.2.1, 6.0, 6.0.1, 6.0.3, 6.1	A buffer overflow vulnerability exists when an excessively long hyperlink to a file resource is embedded in an HTML e-mail, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Eudora Embedded Hyperlink Buffer Overflow	**High**	Bug discussed in newsgroups and websites. A Denial of Service exploit script has been published.
recipants.pants-blazing.com[178]	Windows, Unix	ReciPants 1.0, 1.0.1, 1.1, 1.1.1	Several vulnerabilities exist due to insufficient verification of input passed to various parameters before being used in SQL queries, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrades available at: http://recipants.pantsblazing.com/dist/ReciPants-v1.2.tar.gz	ReciPants SQL Injection and Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Rosiello Security[179]	Multiple	Sphiro HTTPD 0.1 B	A buffer overflow vulnerability exists due to insufficient verification of buffer boundaries before storing input in fixed buffers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Security Sphiro HTTPD Remote Heap Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Royal Institute of Technol-ogy[180] ***FreeBSD issues advisory[181]***	**Unix**	**KTH Heimdal 0.4 a-0.4 e, 0.5-0.5.2, 0.6 .0**	**A vulnerability exists due to an error in the validation of cross-realm requests, which could let a malicious user impersonate anyone in the cross-realm trust path.**	**Upgrades available at: ftp://ftp.pdc.kth.se/pub/heimdal/src/** **Debian:** http://security.debian.org/pool/updates/main/h/heimdal ***FreeBSD:*** **ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:08/heimdal51.patch**	**Heimdal Kerberos Cross-Realm Validation** **CVE Name: CAN-2004-0371**	**Medium**	**Bug discussed in newsgroups and websites.**
Royal Institute of Techno-logy [182]	Unix	KTH Heimdal 0.5-0.5.3, 0.6 .0, 0.6.1	A vulnerability exists due to a pre-authentication flaw in the k5admind(8) Kerberos Key Distribution Center (KDC) interface in the processing of Kerberos 4 compatibility administration requests, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Update available at: ftp://ftp.pdc.kth.se/pub/heimdal/src/heimdal-0.6.2.tar.gz **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:09/kadmind.patch	Heimdal K5AdminD Remote Heap Buffer Overflow CVE Name: CAN-2004-0434	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[177] Secunia Advisory, SA11568, May 7, 2004.
[178] Secunia Advisory, SA11533, May 4, 2004.
[179] SecurityFocus, April 30, 2004.
[180] Debian Security Advisory, DSA 476-1, April 6, 2004.
[181] FreeBSD Security Advisory, FreeBSD-SA-04:08, May 5, 2004.
[182] FreeBSD Security Advisory, FreeBSD-SA-04:09.kadmind, May 5. 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Samsung [183]	Multiple	Smart Ether SS6215S Switch	A vulnerability exists when accessing the switch via the telnet service or serial connection because it is possibly to bypass the authentication procedure, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	SmartEther Switch Authentication Bypass	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
SGI [184]	Unix	IRIX	An undisclosed UDP Denial of Service vulnerability exists.	Patches available at: ftp://patches.sgi.com/	IRIX Unspecified UDP Denial of Service	Low	Bug discussed in newsgroups and websites.
SGI [185]	Unix	IRIX	A vulnerability exists in ifconfig %interface% -arp due to a failure to disable ARP handling, which could lead to a false sense of security.	Patches available at: ftp://patches.sgi.com/	IRIX IFConfig -ARP Failure To Disable ARP Functionality	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Siemens [186]	Multiple	S55	A vulnerability exists due to a race condition during which the Java code can overlay the normal permission request with an arbitrary screen display, which could let a remote malicious user cause a target user's phone to send out SM S messages.	No workaround or patch available at time of publishing.	S55 Cellular Telephone Unauthorized SMS Messages	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Simple Machines [187]	Windows, Unix	SMF 1.0 - beta5p, beta4p, beta4.1	A vulnerability exists due to insufficient filtering of HTML code from user-supplied input in '[size]' tags, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	SMF Size Tag	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
SmartPeer [188]	Multiple	SmartPeer 0.1	A vulnerability exists in the 'smartpeer -p mynewpassword' command..	Upgrade available at: http://www.smartpeer.com/Media/Data/SmartPeer-0.0.2.iso	SmartPeer Undisclosed Local Vulnerability	Medium	Bug discussed in newsgroups and websites.

[183] SecurityTracker Alert, 1009947, April 26, 2004.
[184] SGI Security Advisory, 20050502-01-P, May 5, 2004.
[185] SGI Security Advisory, 20050502-01-P, May 5, 2004.
[186] Securiteam, April 29, 2004.
[187] SecurityTracker Alert, 1010070, May 5, 2004.
[188] SecurityTracker Alert ID: 1010026, May 1, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SMC Networks [189]	Multiple	SMC Broad-band Router SMC7008 ABR (1.032, SMC7004 VBR (1.231)	A vulnerability exists because the default configuration does not set a password, which could let a remote malicious user unauthorized administrative access.	No workaround or patch available at time of publishing.	SMC Broadband Routers Unauthorized Administrative Access	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
South River Technol-ogies [190]	Windows NT	Titan FTP Server 3.01	A remote Denial of Service vulnerability exists when a malicious user executes a 'LIST' command and then disconnects before the command has had time to connect back to the client.	Update available at: http://srt.swmirror.com/titanftp.exe *Note: This is the evaluation version of the software. If you have a licensed copy, there is a 'Check for Program Update' utility available with your installation.*	Titan FTP Server LIST Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Squirrel Mail [191] ***Another exploit script published & upgrade available*** *[192, 193]*	**Imox**	**Squirrel Mail change_ passwd 3.1 -1.2.8**	**A buffer overflow vulnerability exists in the 'change_passwd' plug-in utility due to a boundary error, which could let a malicious user execute arbitrary code.**	***Upgrade available at:*** **http://www.squirrelmail.org/countdl.php?fileurl=http%3A%2F%2Fwww.squirrelmail.org%2Fplugins%2Fchange_passwd-4.0-1.2.8.tar.gz**	**SquirrelMail Change_ Passwd Plug-in Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Exploit scripts have has been published.** ***Another exploit script has been published.***
Squirrel Mail Develop-ment Team [194]	Unix	Squirrel Mail 1.0.4, 1.0.5, 1.2.0-1.2.11, 1.4- 1.4.2	A Cross-Site Scripting vulnerability exists due to an input validation error in 'compose.php' when handling input passed to the 'mailbox' parameter, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	SquirrelMail Folder Name Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

[189] Bugtraq, April 28, 2004.
[190] Securiteam, May 4, 2004.
[191] Bugtraq, April 17, 2004.
[192] Packet storm, May 4, 2004.
[193] SecurityFocus, April 27, 2004.
[194] Bugtraq, April 29, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[195]	Windows, Unix	JRE & SDL (Linux Product-ion Release) 1.4.2 _03, 1.4.2, JRE & SDK (Solaris Produc-tion Release) 1.4.2 _03, 1.4.2, JRE & SDK (Windows Produc-tion Release) 1.4.2 _03, 1.4.2	A remote Denial of Service vulnerability exists in the 'decodeArrayLoop()' function in ISO2022_JP$Decoder.	Upgrades available at: http://java.sun.com/j2se/1.4.2/download.html	Sun Java Runtime Environment Remote Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[196]	Unix	Solaris 8.0, 8.0_x86, 9.0, 9.0_x86	A Denial of Service vulnerability exists when a malicious user invokes the 'ip_sioctl_copyin_done()' function to cause a NULL queue pointer to be passed to the 'putnext()' function.	Patches available at: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57545	Solaris TCP/IP Networking Stack Denial of Service	Low	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[197]	Unix	Sun Patch 113579-02, 113579-03, 113579-04, 113579-05, 114342-02, 114342-03, 114342-04, 114342-05	Sun has announced that some patches released for Solaris may present a new security vulnerability. The issue presents itself in Solaris 9 systems running as NIS servers containing secure maps and patches 113579-02 through 113579-05 (for SPARC) or 114342-02 through 114342-05 (for x86) installed. Successful exploitation of this issue could let a malicious user obtain sensitive information.	Patches available at: http://sunsolve.sun.com/tpatches	Solaris Patch Information Disclosure	Medium	Bug discussed in newsgroups and websites.
SuSE[198]	Unix	Linux 8.1, 9.0, Linux Enterprise Server 8	A Denial of Service vulnerability exists due to improper file permissions on the '/proc/scsi/qla2300/HbaApiNode' file.	Update available at: ftp://ftp.suse.com/pub/suse	Linux Kernel Denial of Service	Low	Bug discussed in newsgroups and websites.

[195] Sun(sm) Alert Notification, 57555, May 6, 2004.
[196] Sun(sm) Alert Notification, 57545, April 23, 2004.
[197] Sun(sm) Alert Notification, 57554, April 30, 2004.
[198] SuSE Security Announcement, SuSE-SA:2004:010, May 5, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SuSE[199]	Unix	LINUX 9.1 Personal Edition CD-ROM	A vulnerability exists because a password is not set for the root account, which could let a remote malicious user obtain root access..	Upgrade available at: ftp://ftp.suse.com/pub/suse/i386/live-cd-9.1/LiveCD-9.1-01.iso	LINUX 9.1 Personal Edition Live CD-ROM SSH Server Remote Root Access	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
The PaX Team[200]	Unix	PaX linux 2.6.5	A Denial of Service vulnerability exists due to an error within the 'mmap()' mechanism when the PaX Address Space Layout Randomization Layout (ASLR) is enabled.	Patch available at: http://pax.grsecurity.net/pax-linux-2.6.5-200405011700.patch	PaX Denial of Service	Low	Bug discussed in newsgroups and websites.
Trend Micro[201]	Windows 95/98/ME/ NT 4.0/2000	Office Scan Corporate Edition 3.0, 3.5, 3.11, 3.13, 3.54, 5.02, 5.58	A vulnerability exists because the default directory and registry permissions are insecure, which could let a malicious user manipulate the registry and contents of the directory. This can be exploited to stop the virus scanning and change the configuration.	No workaround or patch available at time of publishing.	OfficeScan Weak Default Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
University of Cam-bridge[202]	Unix	Exim 3.35, 4.3.2	Two buffer overflow vulnerabilities exist: a vulnerability exists in 'accept.c' (exim 3.35) if the 'headers_check_syntax' option is configured in 'exim.conf,' which could let a remote malicious user execute arbitrary code; and a vulnerability exists in 'verify.c' (exim 4.32) if the 'require verify = header_syntax' option is set, which could let a remote malicious user execute arbitrary code.	**Debian:** http://www.debian.org/security/2004/dsa-501	Exim Remote Buffer Overflows CVE Name: CAN-2004-0399, CAN-2004-0400	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[199] SuSE Security Announcement, SuSE-SA:2004:011, May 6, 2004.
[200] SECUNIA ADVISORY, SA11518, May 4, 2004.
[201] Bugtraq, May 7, 2004.
[202] Debian Security Advisory, DSA-501-1, May 7, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Veritas Software [203]	Unix	Net Backup Profes-sional 3.5, 3.6, 3.51, 3.51.10, 3.51.15, 3.51.20, 3.51.30, Advanced Reporter 3.4, 4.5, FP1- FP4, MP1-MP4, 5.0, Global Data Manager 4.5, FP1-FP4, MP1-MP4, 5.0	Multiple buffer overflow and format string vulnerabilities exist, which could let a remote malicious user execute arbitrary code with root privileges.	No workaround or patch available at time of publishing.	NetBackup Multiple Buffer Overflows & Format String	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Verity Inc.[204]	Windows NT 4.0/2000, Unix	Ultraseek 5.2.1	A vulnerability exists because requests containing reserved DOS device names are handled incorrectly, which could let a remote malicious user obtain sensitive information.	Please contact the vendor to obtain a fixed version.	Ultraseek Reserved DOS Device Name CVE Name: CAN-2004-0050	Medium	Bug discussed in newsgroups and websites.
Web Wiz Guide [205]	Windows	Web Wiz Forums 7.0 beta1, 7.0 1, 7.0, 7.5, 7.7 b, 7.7 a, 7.51	Multiple vulnerabilities exist: a vulnerability exists in the 'pop_up_ip_blocking.asp' script due to insufficient verification of the 'chkDelete' parameter, which could let a remote malicious user execute arbitrary SQL code; a vulnerability exists due to a logic error in 'pop_up_topic_admin.asp,' which could let a remote malicious user manipulate topic status without authentication; and a vulnerability exits due to a logic error in 'pop_up_ip_blocking.asp,' which could let a remote malicious user block arbitrary IP address without authentication.	No workaround or patch available at time of publishing.	Web Wiz Forum Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.

[203] SecurityFocus, April 27, 2004.
[204] Corsaire Security Advisory, May 5, 2004.
[205] Securiteam, May 4, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Xue-brothers[206]	Windows 2000, XP	MyWeb 3.3	A buffer overflow vulnerability exists due to a boundary error within the HTTP request handling, which could let a malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	MyWeb HTTP Server GET Request Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
YaBB[207]	Windows, Unix	YaBB 1 Gold - SP 1.2, SP 1	An input validation vulnerability exists in the 'subject' field, which could let a remote malicious user modify user information.	No workaround or patch available at time of publishing.	YaBB 'Subject' Field Input Validation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Zonet[208]	Multiple	Zonet ZSR1104 WE 2.41	A vulnerability exists because the network address translation function modifies the source address of inbound packets to be the address of the device, making it impossible to perform effective access controls within the internal network.	No workaround or patch available at time of publishing.	Zonet Wireless Router NAT Implementa-tion Design Flaw	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

[206] SP Research Labs Advisory x11, May 6, 2004.
[207] SecurityTracker Alert, 1010036, May 3, 2004.
[208] SecurityFocus, April 27, 2004.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between April 27 and May 11, 2004, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period 46 scripts, programs, and net-news messages containing holes or exploits were identified by US-CERT. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
May 11, 2004	autoRST.c	Script that exploits the Multiple Vendor TCP Sequence Number Approximation vulnerability.
May 10, 2004	xphack.c	Remote exploit for the Windows LSSARV.DLL RPC Buffer Overflow vulnerability.
May 9, 2004	305-pound.c	Script that exploits the Pound Remote Format String vulnerability.
May 9, 2004	auxploit-1.0.tgz	A remote exploitation tool for the c:\aux vulnerability that is able to completely lock a user mail client.
May 9, 2004	**eudoraURL.txt**	**Exploit for the Eudora Embedded Hyperlink Buffer Overflow vulnerability.**
May 9, 2004	gwee-1.21.tar.gz	Generic Web Exploitation Engine, is a small program written in C designed to exploit input validation vulnerabilities in web scripts, such as Perl CGIs, PHP, etc. that features several reverse connecting shellcodes, 4 methods of injection, and a built-in HTTP/HTTPS client and server.
May 9, 2004	knock-0.3.tar.gz	A server/client set of tools that implements the idea known as port-knocking. Port-knocking is a method of accessing a backdoor to your firewall through a special sequence of port hits.
May 9, 2004	msIPSec.txt	Write up that notes how Microsoft's Windows IPSec implementation fails to properly authenticate an IPSec gateway and in return will accept client certificates as gateway certificates.
May 9, 2004	rrs-1.49.tar.gz	A reverse (connecting) remote shell. Instead of listening for incoming connections it will connect out to a listener (rrs in listen mode).
May 9, 2004	sishell-0.1.tar.gz	A reverse (connecting) shellcode kit for x86 Linux, FreeBSD, NetBSD and OpenBSD that generates both regular shellcode without NULLs and stand-alone ELF executables.
May 9, 2004	webrampscan-0.2.tar.gz	The WebRamp scanner is program that scans for open webramp administration webpages, rips the usernames and passwords out, and dumps them into a text file.
May 9, 2004	WFBE.txt	Write up that details how to defeat file browsing restrictions on Windows 98 running Novell 3.2.0.0.
May 9, 2004	win_msrpc_lsass_ms04-11_Ex.c	Remote exploit for the Windows LSSARV.DLL RPC Buffer Overflow vulnerability.
May 9, 2004	x25bru.c	Multithreaded multi-link X.25 Pad password brute-forcing utility.
May 8, 2004	**sp-myweb3.3.c**	**Proof of Concept exploit for the MyWeb HTTP Server GET Request Buffer Overflow vulnerability.**
May 7, 2004	**eudora_url_dos.pl**	**Perl Denial of Service exploit for the Eudora Embedded Hyperlink Buffer Overflow vulnerability.**
May 7, 2004	exim1.html	Proof of Concept exploit for the Exim Remote Buffer Overflow vulnerabilities.
May 7, 2004	gyan_sendmail.c	Local root exploit for Sendmail Prescan Function vulnerability.

Date of Script (Reverse Chronological Order)	Script name	Script Description
May 7, 2004	phpx326.txt	Proof of Concept exploit for the PHPX Multiple Cross-Site Scripting vulnerabilities.
May 5, 2004	4nalb.pl	Remote exploit that makes use of a file inclusion vulnerability in 4nalbum module.
May 5, 2004	**bpexploit.pl**	**Perl script that exploits the NetBackup Multiple Buffer Overflows & Format String vulnerabilities.**
May 5, 2004	**netbkup.pl**	**Perl script that exploits the NetBackup Multiple Buffer Overflows & Format String vulnerabilities.**
May 5, 2004	**Veritas_multi.pl**	**Perl script that exploits the NetBackup Multiple Buffer Overflows & Format String vulnerabilities.**
May 4, 2004	autoRST.c	An automated TCP RST exploit that uses the Winpcap libraries to sniff for TCP packets on a network and then sends out a forged RST packet after calculating the appropriate sequence number and forging the MAC address.
May 4, 2004	dwgenkey.c	Exploit for the Dameware's Mini Remote Control System Weak Key Agreement Scheme vulnerability.
May 4, 2004	sq-chpass-exp.c	Script that exploits the SquirrelMail Change_ Passwd Plug-in Buffer Overflow vulnerability.
May 4, 2004	SSLPCT.txt	White paper analysis of the SSL PCT vulnerability that gives full details on how exploitation has been performed and what it took for working exploits to be created.
May 4, 2004	titan_ftp_dos.pl	Perl exploit for the Titan FTP Server LIST Denial of Service vulnerably.
May 4, 2004	xxchat-socks5.c	Script that exploits the XChat SOCKS 5 Remote Buffer Overflow vulnerability.
May 2, 2004	lha.c	Proof of Concept exploit for the LHA Buffer Overflow/ Directory Traversal Vulnerabilities.
May 2, 2004	overflow.lha.uuc.gz	Proof of Concept exploit for the LHA Buffer Overflow/ Directory Traversal Vulnerabilities.
May 1, 2004	04252004.ms04011lsass.c	Remote exploit for the Windows LSSARV.DLL RPC Buffer Overflow vulnerability.
May 1, 2004	aexpl-1.0.tar.gz	AntiExploit is a small Perl script that scans for well known exploit files. It currently recognizes over 1400 suspicious files, and the database is updated weekly.
May 1, 2004	cge-13.tar.gz	Cisco Global Exploiter is a tool that demonstrates exploitation of the multiple Cisco vulnerabilities.
May 1, 2004	HOD-ms04011-lsasrv-expl.c	Remote exploit for the Windows LSSARV.DLL RPC Buffer Overflow vulnerability.
May 1, 2004	hsftpexpl.tgz	Exploit for the HSFTP Format String Vulnerability.
May 1, 2004	hydra-4.0-palm.zip	A high quality parallelized login hacker for Samba, Smbnt, Cisco AAA, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more.
May 1, 2004	lboeg.pl.txt	Local buffer overflow exploit generator for Linux, BSD, BSDi, HP-UX, UnixWare, IRIX and SCO.
May 1, 2004	plem.tar.gz	Perl Loadable Exploiting Module (PLEM) is an advanced module for Perl programming that provides a list of common functions for local and remote exploit coding.
April 28, 2004	Rose_Frag_Attack_Explained.txt	Updated version of the white-paper discussing the Rose Attack method and how sending two parts of a fragmented packet can cause various outcomes to network devices, including Denial of Service problems.
April 28, 2004	RoseAttackv1.txt	A program that demonstrates the Rose Attack eating up CPU processing time on a Windows 2000 box..
April 28, 2004	RoseAttackv2.txt	A program that demonstrates the Rose Attack eating up CPU processing time on a Windows 2000 box..

Date of Script (Reverse Chronological Order)	Script name	Script Description
April 28, 2004	ssdt-0.1.tar.gz	The SSDT utility makes use of sending spoofed ICMP and UDP traffic to send RSA encrypted files. Both client and server side programs are included.
April 27, 2004	jetadmin_exp.pl	Perl script that exploits the Jetadmin Root Access vulnerability.
April 27, 2004	priv8lcd.pl	Perl script that exploits the LCDd Multiple Remote Vulnerabilities.
April 27, 2004	**siemensS55JavaSMSExploit.java**	**Exploit for the S55 Cellular Telephone SMS Confirmation Message Bypass vulnerability.**

Trends

- **US-CERT has received reports of a new worm, referred to as "W32/Sasser." This worm attempts to take advantage of a buffer overflow vulnerability in the Windows Local Security Authority Service Server (LSASS). See Microsoft Security Bulletin located at: http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx. The vulnerability allows a remote malicious user to execute arbitrary code with SYSTEM privileges. There are several variants of this worm circulating in the wild. For more information, see US-CERT Activity located at: http://www.us-cert.gov/current/current_activity.html.**
- **Fraudulent e-mails designed to dupe Internet users out of their credit card details or bank information topped the three billion mark last month, according to one of the largest spam e-mail filtering companies. The authentic-looking e-mails, masquerading as messages from banks or online retailers, have become a popular new tool for tech-savvy fraudsters in a new scam known as "phishing."**
- **US-CERT is aware of network activity that is consistent with scanning and/or exploit attempts against the buffer overflow vulnerability in the Microsoft Private Communication Technology (PCT) protocol, which was remedied by the patches described in Microsoft Security Bulletin MS04-011. Reports indicate increased network traffic to ports 443/tcp and 31337/tcp. For more information, see US-CERT Activity located at: http://www.us-cert.gov/current/#pct.**
- **US-CERT is aware of exploitation of a cross-domain scripting vulnerability in the Outlook Express MIME Encapsulation of Aggregate HTML Documents (MHTML) protocol handler, which was remedied by the patches described in Microsoft Security Bulletin MS04-013. This vulnerability appears to be exploited by the Ibiza Trojan, W32/Bugbear.E, and various web sites that host malicious URLs and related malware. For more information, see US-CERT Activity located at: http://www.us-cert.gov/current/#pct.**
- **US-CERT is aware of exploitation of a cross-domain scripting vulnerability in the InfoTech Storage (ITS) protocol handlers used by Microsoft Internet Explorer (IE). By convincing a victim to view an HTML document (web page, HTML e-mail), a malicious user could execute arbitrary code with the privileges of the user running IE and read or modify content in another web site. For more information see US-CERT Current Activity located at: http://www.us-cert.gov/current/current_activity.html.**
- **US-CERT is aware of a new mass-mailing malicious code known as "Sober.F." Sober.F arrives as an e-mail message written in German or English and containing a 42,496-byte e-mail attachment. For more information see US-CERT Current Activity located at: http://www.us-cert.gov/current/current_activity.html.**
- **Exploit code has been publicly released that takes advantage of multiple vulnerabilities in various Cisco products. For more information see US-CERT Current Activity located at: http://www.us-cert.gov/current/current_activity.html.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. NOTE: At times, viruses may contain names or content that may be considered offensive.

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, and The WildList Organization International.

VBS_GEDZA.A (Aliases: VBS.Gaggle.D, VBS/Gedza, I-Worm.Gedza, VBS/Lefarsi.A) (Visual Basic Script Worm): This destructive Visual Basic script file displays a picture of the popular Canadian singer, Avril Lavigne, when it is executed. Depending on the value of the current system day, it may drop a file, display messages or open the Avril Lavigne Web site. It also infects .XLS and .DOC files, and overwrites or appends itself to files with specific extensions. It propagates via peer-to-peer file sharing networks by dropping copies of itself in a peer-to-peer shared folders, using interesting file names to entice users to download the files. It also propagates via Outlook Express by changing its stationary with a dropped worm copy. It runs on Windows 98, ME, NT, 2000 and XP.

VBS/Yarr-B (Visual Basic Script Worm): This worm drops the W32/Mimail-V worm as the file c:\temp\gorf.ex0.

W32/Agobot-GJ (Aliases: Backdoor.Agobot.oi, W32/Gaobot.worm.gen.f, W32.HLLW.Gaobot.gen) (Win32 Worm): This is a member of the W32/Agobot family of worms for the Windows platform. In order to run automatically when Windows starts up W32/Agobot-GJ copies itself to the file regsvs.exe in the Windows system folder and creates the following registry entries pointing to this file:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Compatibility Service Process = regsvs.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Compatibility Service Process=regsvs.exe

W32/Agobot-GJ also allows a malicious user remote access to an infected computer via the IRC network.

W32/Agobot-HD (Win32 Worm): This is an IRC backdoor Trojan and network worm. It is capable of spreading to computers on the local network protected by weak passwords. When first run,W32/Agobot-HD copies itself to the Windows system folder as wmiprvsw.exe and creates the following registry entries to run itself on startup:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run System Updater Service = wmiprvsw.exe
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices system Updater Service = wmiprvsw.exe

Each time W32/Agobot-HD is run, it attempts to connect to a remote IRC server and join a specific channel. W32/Agobot-HD then runs continuously in the background, allowing a remote intruder to access and control the computer via IRC channels. W32/Agobot-HD attempts to terminate and disable various anti-virus and security-related programs. It also includes a stealthing component which attempts to hide the worm.

W32/Agobot-NA (Aliases: Backdoor.Agobot.gen, W32/Gaobot.worm.gen.j, W32.HLLW.Gaobot.gen) (Win32 Worm): This is a backdoor Trojan and worm which spreads to computers protected by weak passwords. When first run, W32/Agobot-NA copies itself to the Windows system folder as wmiprvsw.exe and creates the following registry entries to run itself on startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\System Updater Service = wmiprvsw.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\System Updater Service = wmiprvsw.exe

The worm runs continuously in the background providing backdoor access to the computer. W32/Agobot-NA attempts to terminate and disable various anti-virus and security-related programs. It also modifies the HOSTS file located at %WINDOWS%\System32\Drivers\etc\HOSTS, mapping selected anti-virus websites to the loopback address 127.0.0.1 in an attempt to prevent access to these sites. It will also attempt to retrieve data from various websites.

W32/Agobot-PV (Aliases: Backdoor.Agobot.pv, W32.HLLW.Gaobot.gen, WORM_AGOBOT.GEN) (Win32 Worm): This is an IRC backdoor Trojan and network worm. It is capable of spreading to computers on the local network protected by weak passwords. When first run, W32/Agobot-PV moves itself to the Windows system folder as pb.exe and creates the following registry entries to run itself on startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WSAConfiguration = pb.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\WSAConfiguration = pb.exe

Each time the Trojan is run it attempts to connect to a remote IRC server and join a specific channel. The Trojan then runs continuously in the background, allowing a remote intruder to access and control the computer via IRC channels. It also attempts to terminate and disable various anti-virus and security-related programs and modifies the HOSTS file located at %WINDOWS%\System32\Drivers\etc\HOSTS, mapping selected anti-virus websites to the loopback address 127.0.0.1 in an attempt to prevent access to these sites.

W32/Agobot-VB (Aliases: Backdoor.Agobot.gen, W32/Gaobot.worm.gen.j, W32.Gaobot.AFJ) (Win32 Worm): This is a backdoor Trojan and worm which spreads to computers protected by weak passwords. When first run, W32/Agobot-VB copies itself to the Windows system folder as uu.exe and creates the following registry entries to run itself on startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\yx=uu.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\yx=uu.exe

The Trojan runs continuously in the background providing backdoor access to the computer. It attempts to terminate and disable various anti-virus and security related programs and modifies the HOSTS file located at %WINDOWS%\System32\Drivers\etc\HOSTS, mapping selected anti-virus websites to the loopback address 127.0.0.1 in an attempt to prevent access to these sites. W32/Agobot-VB queries various websites to test internet connectivity.

W32.Arcam (Win32 Virus): This is a virus that attempts to infect the .exe, .cpl, and .scr files. It may also attempt to spread by e-mail and IRC. Due to corruption, the only known samples of this virus did not successfully propagate. W32.Arcam copies itself as C:\Secret.txt.exe and drops the file, C:\plaeCBBNV.vbs. This file contains commands to e-mail the worm to all the contacts in the Outlook address book. If it succeeds, the e-mail will have the following characteristics:

- Subject: Test
- Attachment: secret.txt.exe
- Message: test

W32.Axon (Aliases: W32/Riaz, Win32.HLLP.Xenon) (Win32 Virus): This is a simple virus that prepends itself to the files with the .exe extension. It also deletes the files with .mp3 and .avi extensions.

W32.Axon.B (Alias: Win32.HLLP.Riaz) (Win32 Virus): This is a virus that prepends itself to the files with the .exe extension. It also deletes the files with .mp3 and .avi extensions.

W32/Bagle-AA (Aliases: Win32/Bagle.AB, WORM_BAGLE.Z, I-Worm.Bagle.z) (Win32 Worm): This worm has been reported in the wild. It is a member of the W32/Bagle family of worms. When first run, W32/Bagle-AA will display a fake error message containing the text "Can't find a viewer associated with the file." W32/Bagle-AA copies itself to the Windows system folder with the filename drvddll.exe and then runs the worm from that location. The e-mail sent by the worm various subject lines. The following registry entry is created so that the worm is run when a user logs on to Windows:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\drvddll.exe = drvddll.exe

W32/Bagle-AA scans all fixed drives recursively for WAB, TXT, MSG, HTM, SHTM, STM, XML, DBX, MBX, MDX, EML, NCH, MMF, ODS, CFG, ASP, PHP, PL, WSH, ADB, TBB, SHT, XLS, OFT, UIN, CGI, MHT, DHTM, and JSP files, extracts e-mail addresses from them and uses those addresses for the mass mailing

component of the worm. The worm will create copies of itself with various filenames in folders that contain the string "shar" in their name and attempts to terminate various processes.

W32/Bugbear-F (Aliases: I-Worm.Tanatos.e, W32/Bugbear.gen@MM, W32.Bugbear.E@mm, WORM_BUGBEAR.D, WORM_BUGBEAR.F) (Win32 Worm): This worm has been reported in the wild. It is a worm which spreads via e-mail. The subject line and attached file of the e-mail sent by the worm are variable and may be taken from information on the infected computer. The attached file has an extension of ZIP. W32/Bugbear-F creates a copy of itself with a randomly generated name in the Windows system folder. To ensure that the copy of the worm is run each time Windows is started the worm adds a randomly named value to the registry key:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

The worm creates several other files with random names in the Windows system folder. One of the files is a DLL used to monitor the user's keystrokes. W32/Bugbear-F terminates various anti-virus and security related processes.

W32/Bugbear-G (Aliases: W32.Bugbear.E@mm, W32/Bugbear.gen@MM virus) (Win32 Worm): This is a worm which spreads via e-mail. The subject line and attached file of the e-mail sent by the worm are variable and may be taken from information on the infected computer. The attached file has an extension of PIF. It creates a copy of itself with a randomly generated name in the windows system folder. To ensure that the copy of the worm is run each time Windows is started the worm adds a randomly named value to the registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

The worm creates several other files with random names in the Windows system folder. One of the files is a DLL used to monitor the user's keystrokes. It terminates various anti-virus and security related processes.

W32/Famus-C (Aliases: W32/Misodene.gen@MM virus, Win32/Liber.A worm) (Win32 Worm): This worm has been reported in the wild. It will make an additional copy of itself as Red7324.exe in the Temp folder along with other files which are used for mailing the worm. Among these will be the file SMTP.OCX which is a freeware SMTP engine used in the mailing of W32/Famus-C to e-mail addresses found on the computer. Other dropped files include:

- C:/En Cuba no hay libertad de expresion - an empty file
- <Windows>/temp/Casper9247.exe - used by the worm
- <Windows>/temp/att1.att1 - contains the e-mail's file attachment name
- <Windows>/temp/msg.msg - contains the e-mail's message text
- <Windows>/temp/sub.sub - contains the e-mail's subject line

The e-mail sent by the worm will have the following characteristics:

- Subject line: Famous / Famosos
- Attachment: Famous.exe

Another e-mail may also be sent out without a copy of the worm with the following characteristics:

- Subject line: Virus Infected!!!!

W32/Famus-C will also display a message box displaying the text above on the infected computer.

W32.Gobot.A (Aliases: Backdoor.Gobot.u, Exploit-Mydoom) (Win32 Worm): This is a worm that spreads through IRC, open network shares, and file-sharing networks. The worm also propagates through any backdoors installed by the Mydoom family of worms. It is written in Borland Delphi programming language and may be compressed with UPX.
Also Known As:

W32.Gaobot.AFC (Win32 Worm): This is a worm that spreads through open network shares and several Windows vulnerabilities including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445. Windows XP users are protected against this vulnerability if Microsoft Security Bulletin MS03-043 has been applied. Windows 2000 users must apply MS03-049.

- The UPnP vulnerability (described in Microsoft Security Bulletin MS01-059).
- The vulnerabilities in the Microsoft SQL Server 2000 or MSDE 2000 audit (described in Microsoft Security Bulletin MS02-061) using UDP port 1434.
- Exploits the Microsoft Windows Local Security Authority Service Remote Buffer Overflow (described in Microsoft Security Bulletin MS04-011).

The worm also spreads through backdoors that the Beagle and Mydoom worms and the Optix family of backdoors install. The worm can also act as a backdoor server program and attack other systems. Additionally, the worm attempts to stop the process of many antivirus and security programs.

W32.Gaobot.AFW (Win32 Worm): This is a worm that spreads through open network shares and several Windows vulnerabilities including:

- The DCOM RPC Vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135.
- The WebDav Vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80.
- The Workstation Service Buffer Overrun Vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445. Windows XP users are protected against this vulnerability if Microsoft Security Bulletin MS03-043 has been applied. Windows 2000 users must apply MS03-049.
- The UPnP NOTIFY Buffer Overflow Vulnerability (described in Microsoft Security Bulletin MS01-059).
- The vulnerabilities in the Microsoft SQL Server 2000 or MSDE 2000 audit (described in Microsoft Security Bulletin MS02-061) using UDP port 1434.
- Exploits the Microsoft Windows Local Security Authority Service Remote Buffer Overflow (described in Microsoft Security Bulletin MS04-011).

The worm also spreads through backdoors that the Beagle and Mydoom worms and the Optix family of backdoors install. W32.Gaobot.AFW can act as a backdoor server program and attack other systems. It attempts to kill the processes of many antivirus and security programs .

W32/Agobot-QA (Aliases: Backdoor.Agobot.gen, W32/Polybot.gen!irc, W32.Gaobot.gen!poly) (Win32 Worm): This is an IRC backdoor Trojan and network worm which establishes an IRC channel to a remote server in order to grant an intruder access to the compromised machine. This worm will move itself into the Windows System32 folder under the filename SYSTEMC.EXE and may create the following registry entries so that it can execute automatically on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SysStrt = systemc.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\SysStrt = systemc.exe

The following registry branches will also be created:

- HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SYSTEM_START\
- HKLM\SYSTEM\CurrentControlSet\Services\System Start\

W32/Agobot-QA may also attempt to collect e-mail addresses from the Windows Address Book and send itself to these e-mail addresses using its own SMTP engine with itself included as an executable attachment. W32/Agobot-QA may attempt to terminate anti-virus and other security-related processes, in addition to other viruses, worms or Trojans. W32/Agobot-QA may search for shared folders on the internet with weak passwords and copy itself into them. A text file named HOSTS in C:\<Windows System32>\drivers\etc\ may be created or overwritten with a list of anti-virus and other security-related websites, each bound to the IP loopback address of 127.0.0.1 which would effectively prevent access to these sites. It can sniff HTTP, ICMP, FTP and IRC network traffic and steal data from them. The following vulnerabilities can also be exploited to aid propagation on unpatched systems and manipulate registry keys:

- Remote Procedure Call (RPC) vulnerability
- Distributed Component Object Model (DCOM) vulnerability
- RPC Locator vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability

W32/Agobot-QA can also polymorph on installation in order to evade detection and share / delete the admin$, ipc$ etc drives.

It can also test the available bandwidth by attempting to GET or POST data to various websites. W32/Agobot-QA can also be used to initiate denial-of-service (DoS) and distributed Denial of Service synflood/httpflood/fraggle/smurf attacks against remote systems. This worm can steal the Windows Product ID and keys from several computer applications or games.

W32.Donk.Q (Win32 Worm): This is a worm that spreads through open network shares and attempts to exploit the Microsoft DCOM RPC vulnerability (as described in Microsoft Security Bulletin MS03-026).

The worm can also open a backdoor on an infected computer.
W32.Golo.A@mm (Win32 Worm): This is a simple mass mailing worm. It typically arrives as an e-mail message with the following properties:

- From: webmaster@<recipient's domain>
- Subject: <configurable>
- Attachment: navupdate.exe
- Message Body: <configurable>

W32/Netsky-AA (Aliases: W32/Netsky.aa@MM virus, INFECTED I-Worm.NetSky.ab) (Win32 Worm): This is a mass mailing worm. When started the worm copies itself to the Windows folder using the name winlogon.scr and sets the following registry entry to auto start on user logon:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SkynetsRevenge = <WINDOWS>\winlogon.scr

It will harvest e-mail addresses from files on any fixed drives with the following extensions: EML, TXT, PHP, CFG, MBX, MDX, ASP, WAB, DOC, VBS, RTF, UIN, SHTM, CGI DHTM, ADB, TBB, DBX, PL, HTM, HTML, SHT, OFT, MSG, ODS, STM, XLS, JSP, WSH, XML, MHT, MMF, NCH, and PPT. The subject lines, message texts and attachments are constructed randomly from various building blocks.

W32/Netsky-AB (Aliases: WORM_NETSKY.AB, Win32.Netsky.AB, W32.Netsky.AB@mm, W32/Netsky.ab@MM, NetSky.AB) (Win32 Worm): This worm has been reported in the wild. It is a mass mailing worm that uses its own SMTP engine to e-mail itself to addresses harvested from files on local drives. In order to run automatically when the user logs on to the computer the worm copies itself to the file csrss.exe in the Windows folder and creates the following registry entry to point to it:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\BagleAV

The worm will delete registry entries under this key that point to files named drvsys.exe and ssgrate.exe. These are copies of files related to the Bagle family of worms that may have been dropped by previous infections. It will also gather information about infected systems in a log file called C:\Detlog.txt. E-mails have various subject lines, message texts, and attachments. W32/Netsky-AB will attempt to terminate antivirus-related processes whose filenames contain text taken from a list. The worm will try to establish a connection with various addresses and harvests e-mail addresses from files with the following extensions: ppt, nch, mmf, mht, xml, wsh, jsp, xls, stm, ods, msg, oft, sht, html, htm, pl, dbx, tbb, adb, dhtm, cgi, shtm, uin, rtf, vbs, doc, wab, asp, mdx, mbx, cfg, php, txt, and eml. W32/Netsky-AB contains the text 'Hey Bagle, feel our revenge!.

W32/Netsky-AC (Aliases: W32.Netsky.AC@mm, WORM_NETSKY.AC, Win32.Netsky.AC, I-Worm.NetSky.ad) (Win32 Worm): This worm has been reported in the wild. It is a mass mailing worm. The worm copies itself to the Windows folder as comp.cpl and creates a helper component wserver.exe in the same folder. W32/Netsky-AC sets the following registry entry to ensure it is run on user logon:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\wserver = wserver.exe

E-mails sent by W32/Netsky-AC have the following characteristics:

- Subject line: Escalation
- Attachment Name: Fix_<virus name>_<random number>.cpl

Sophos researchers have also discovered that hidden inside the code of Netsky-AC is the following text, directed towards anti-virus companies.

> Hey, av firms, do you know that we have programmed the sasser virus?!?. Yeah thats true! Why do you have named it sasser? A Tip: Compare the FTP-Server code with the one from Skynet.V!!! LooL! We are the Skynet...

W32.Randex.AEV (Aliases: W32/Sdbot.worm.gen.j, WORM_SDBOT.Z) (Win32 Worm): This is a network-aware worm that tries to connect to a predetermined IRC server. If this worm is successful, it will wait for instructions from the malicious user. W32.Randex.AEV is written in Microsoft Visual C++, and is packed with UPX and Morphine.

W32/Sasser-A (Aliases: W32/Sasser.worm, Win32/Sasser.A, W32.Sasser.Worm, WORM_SASSER.A, Sasser, Win32.Sasser.A) (Win32 Worm): This worm has been reported in the wild. It is a self-executing network worm, which travels from infected machines via the internet, exploiting a Microsoft Windows vulnerability MS04-011, and instructs vulnerable systems to download and execute the viral code. It does not spread via e-mail. Infected computers may run more slowly than normal and shut down intermittently. W32/Sasser-A attempts to connect to computers through ports TCP/9996 and TCP/445. If the Windows computers are not patched against the LSASS vulnerability, an FTP script is downloaded and executed, which connects to port 5554 and downloads a copy of the worm via FTP (File Transfer Protocol). The worm copies itself to the Windows folder with the filename avserve.exe and sets the following registry key to auto-start on user logon:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\avserve = avserve.exe

The Microsoft vulnerability was first reported on 13 April, and Microsoft have issued protection, which can be downloaded from Microsoft Security Bulletin MS04-011.

W32/Sasser-B (Aliases: WORM_SASSER.B, W32/Sasser.worm.b, W32.Sasser.B.Worm, WORM_SASSER.B, Worm.Win32.Sasser.b, Win32.Sasser.B, Sasser.B, Win32/Sasser.B.worm, W32/Sasser.B) (Win32 Worm): This worm has been reported in the wild. It is a network worm which spreads by exploiting the Microsoft LSASS vulnerability on port 445. For further information on this vulnerability see Microsoft Security Bulletin MS04-011. When first run, W32/Sasser-B copies itself to the Windows folder as avserve2.exe and creates the following registry entry, so that avserve2.exe is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\avserve2.exe = %WINDOWS%\avserve2.exe

A harmless text file is created in the C:\ root folder named win2.log.

W32.Sasser.C.Worm (Aliases: W32/Sasser-C, Worm.Win32.Sasser.c, W32/Sasser.worm.c, WORM_SASSER.C, Win32.Sasser.C) (Win32 Worm): This is a minor variant of W32.Sasser..Worm. It attempts to exploit the LSASS vulnerability described in Microsoft Security Bulletin MS04-011 and spreads by scanning randomly selected IP addresses for vulnerable systems. W32.Sasser.C.Worm differs from W32.Sasser.Worm as follows:

- Uses a different mutex: JumpallsNlsTillt
- Launches 1024 threads (instead of 128).
- Uses a different file name: avserve2.exe.
- Has a different MD5.
- Creates a different value in the registry: "avserve2.exe."

W32.Sasser.C.Worm can run on (but not infect) Windows 95/98/Me computers. Although these operating systems cannot be infected, they can still be used to infect vulnerable systems that they are able to connect to. In this case, the worm will waste a lot of resources so that programs cannot run properly, including our removal tool. (On Windows 95/98/ME computers, the tool should be run in Safe mode.)

W32/Sasser-D (Alias: WORM_SASSER.D, W32.Sasser.D, W32/Sasser.worm.d, Win32.Sasser.D, Worm.Win32.Sasser.d) (Win32 Worm): This worm has been reported in the wild. It is a network worm which spreads by exploiting the Microsoft LSASS vulnerability on port 445. For further information on this vulnerability see Microsoft Security Bulletin MS04-011. When first run W32/Sasser-D copies itself to the Windows folder with the filename skynetave.exe and creates the following registry entry, so the worm is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\skynetave.exe = %WINDOWS%\skynetave.exe

A harmless text file is created in the C:\ root folder named win2.log.

W32/Sasser-E (Aliases: WORM_SASSER.E, W32/Sasser.worm.e, W32.Sasser.E.Worm, Sasser.E) (Win32 Worm): This worm variant contains similar routines as the earlier variants, except for the following unique characteristics:

- The file name of its dropped copy is LSASSS.EXE.
- It uses port 1023 instead of port 5554 and port 1022 instead of port 9996.

It exploits the Windows LSASS vulnerability, which is a buffer overrun that allows remote code execution and enables a malicious user to gain full control of the infected system. To propagate, it scans for vulnerable systems at TCP port 445 and sends a specially-crafted packet to produce a buffer overflow on LSASS.EXE. The packet runs a remote shell that opens port 1022. This worm commands the remote shell to download its copy from the original infected source via port 1023 using FTP. This worm can cause LSASS to crash and force Windows to restart.

W32/Sasser-F (Aliases: Worm.Win32.Sasser.a, W32.Sasser.Worm, W32/Sasser.worm.f) (Win32 Worm): This is a network worm which spreads by exploiting a Microsoft LSASS vulnerability. It copies itself to the Windows folder as NAPATCH.EXE and sets the following registry entry to auto-start on user logon:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\nvpatch = napatch.exe

W32/Sasser-F attempts to connect to random IP addresses on ports TCP/445 and TCP/9996 and then exploit the LSASS vulnerability. If successful an FTP script is uploaded to and executed on the remote computer which then connects back on port 5554 to download a copy of the worm via FTP. W32/Sasser-F may cause the program LSASS.EXE to terminate which generally prompts Windows to shutdown and reboot. However W32/Sasser-F attempts to prevent a system shutdown.

W32/Sdbot-HX (Aliases: Backdoor.IRCBot.gen, W32/Sdbot.worm.gen.n) (Win32 Worm): This is a worm which attempts to spread to remote network shares. It also contains backdoor Trojan functionality, allowing unauthorized remote access to the infected computer via IRC channels while running in the background as a service process. W32/Sdbot-HX copies itself to the Windows system folder as DLL6DSYS.EXE and creates entries in the registry at the following locations to run itself on system startup:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run

W32/Sdbot-HX spreads to network shares with weak passwords as a result of the backdoor Trojan element receiving the appropriate command from a remote user, copying itself to the file PAYLOAD.DAT on the local machine at the same time.

W32/Sdbot-IH (Win32 Worm): This is a network worm and backdoor Trojan. The worm spreads by copying itself to network shares that have weak passwords. The worm creates a copy of itself named bot.exe in the Windows system folder and adds the following registry entries to ensure that the copy is run each time Windows starts:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Synchronization Manager = bot.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Synchronization Manager = bot.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Synchronization Manager = bot.exe

W32/Sdbot-IH maintains a log of the user's keystrokes in a file named keylog.txt in the Windows system folder. The backdoor component of the worm attempts to connect to an IRC server and awaits commands from a remote malicious user.

W32/Sdbot-JT (Aliases: W32/Sdbot.worm.gen.j virus, W32.Randex.gen) (Win32 Worm): This is a member of the W32/Sdbot family of worms. W32/Sdbot-JT copies itself to the Windows system folder as nmsmtp32.exe and sets the following registry entries to ensure it is run at system logon:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Windows driver update = <SYSTEM>\nmsmtp32.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Windows driver update = <SYSTEM>\nmsmtp32.exe

W32.Supova.Z@mm (Win32 Worm): This is a mass mailing worm that sends itself to the e-mail addresses in the Microsoft Outlook address book. The worm also uses IRC to spread. The e-mail has the following characteristics:

- Subject: This document is interesting
- Body: Hi! How are you, I hope all okay. I send you an attachment that you should see.
- Attachment: ha ha ha ha.doc.exe

W32.Supova.Z@mm is written in Microsoft Visual Basic.

W32.Traxg@mm (Win32 Worm): This is a mass-mailing worm that sends itself to e-mail addresses in the Microsoft Outlook address book. The worm is written in Visual Basic.

W32/Vavico.worm (Win Worm): This is a local floppy worm. It doesn't spread by e-mail/network drives. When executed, it displays a fake error message that the file is not a valid windows application. In the meantime it performed malicious actions. A message might appear: "Your pc is vicious___83...! -cjbprog,...By @DhieSoft-. A visual aspect might be the displaying of a bitmap file of the dropped c:\winnt\x-logo.bmp. On the desktop files are put, for example, but not limited to:

- Shakira.mp3.exe
- Download.zip.exe
- Freebsd.doc.exe

It tries to copy itself to the floppy (A:\) drive:

- Sexy.bmp.exe
- Pikachu.bmp.exe
- Linux.doc.exe
- Antidebug.rar.exe
- Ebooks.pdf.exe

It drops files to the root of the C: drive:

- Bios.doc.exe
- Christina Aguilera I turn to you.mp3.exe
- Funny.bmp.exe
- Password.mdb.exe

It also creates files in the %windows system32 directory:

- Eax.exe
- Msvrt.exe
- Term32.exe

It creates files in the %windows directory:

- Exploder.exe
- Krnl836.exe
- Run.exe

It creates a directory with: C:\Program Files\Norton Antivirus\navw32.exe, a directory with: C:\winnt\pc-health\pcguard.exe, and a directory with: C:\winnt\installer\temp\shakira.mp3.mp3. It creates a registry key HKCU\Control Panel\Desktop "scrnsave.exe" with the data set to : C:\winnt\system32\3d_papa_buzzie.scr. It creates a registry key under HKLM\Software\Microsoft\Windows\CurrentVersion\Run with values:

- "Norton Antivirus" and points to the above navw32.exe file
- "Kernel32" and points to the above krnl836.exe file
- "Terminal Services" and points to the above term32.exe file

It puts under HKLM\Software\Microsoft\Command Processor "Autorun" the new data : echo off!copy c:\winnt\config\driver.idf c:\mario.exe|cls|echo.___vicious83(...by Buggie-haeza-tsu). It tries to interfere with AV software. (McAfee,PCCillin,Norton,Panda).

W32.Welchia.K (Win32 Worm): This is a worm that spreads by exploiting Windows vulnerabilities. It is similar to W32.Welchia.D.Worm. W32.Welchia.K uses the following vulnerabilities:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135. The worm specifically targets Windows XP machines using this exploit.

- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80. The worm specifically targets machines running Microsoft IIS 5.0 using this exploit. The worm's use of this exploit will impact Windows 2000 systems and may impact Windows NT/XP systems.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445.
- The Locator service vulnerability using TCP port 445 (described in Microsoft Security Bulletin MS03-001). The worm specifically targets Windows 2000 machines using this exploit.
- The Mydoom backdoor (port 3127).

If the operating system of an infected computer is Chinese, Korean, or English, the worm will attempt to download and install security patches from the Microsoft Windows Update Web site to patch these vulnerabilities. The worm also attempts to remove the W32.Mydoom.A@mm, W32.Mydoom.B@mm, W32.HLLW.Doomjuice, and W32.HLLW.Doomjuice.B worms. The presence of the file %System%\drivers\svchost.exe is an indication of a possible infection.

W97M.Smey (Aliases: W97M/Generic, macro.Word97.Smyser.b) (Word 97 Macro Virus): This is a macro virus that also drops a Trojan horse file. If the Trojan runs, it modifies the MBR of the primary hard drive. Once this happens, you will not be able to boot the computer.

WORM_AGOBOT.HA (Internet Worm): This worm propagates via network shares. It uses the NetBEUI functions to get available lists of user names and passwords. It lists down the available network shares and uses the gathered user names and passwords to access the shares. It also tries to access the shares using a predefined list of user names and passwords. This malware also scans the network for systems vulnerable to the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

The worm also has backdoor capabilities and may execute malicious commands on the host machine. It terminates antivirus-related processes and steals the CD keys, serial numbers, and product IDs of certain applications.

WORM_AGOBOT.IM (Internet Worm): This memory-resident malware has both worm and backdoor capabilities. Like many AGOBOT variants, this worm exploits the Windows LSASS Vulnerability (MS04-11). This is a buffer overrun vulnerability that allows remote code execution. Once successfully exploited, a remote malicious user is able to gain full control of the affected system. For more information about this vulnerability, refer to the following Microsoft Web site:

- MS04-011_MICROSOFT_WINDOWS
  http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

It attempts to log into systems using a list of user names and passwords. It connects to an Internet Relay Chat (IRC) server and joins an IRC channel to listen for remote commands. It allows a remote user to execute malicious commands on the infected system. It also terminates antivirus-related processes and steals CD keys of certain game applications. It runs on Windows 2000 and XP.

WORM_AGOBOT.JF (Aliases: Backdoor.Agobot.gen, WORM_AGOBOT.JO, W32.Gaobot.AFJ, W32/Gaobot.PX.worm , Win32.Agobot.TU, W32/Gaobot.worm.ali) (Internet Worm): This worm is the first known AGOBOT variant to exploit the Windows LSASS Vulnerability (MS04-11), which is a buffer overrun vulnerability that allows remote code execution and enables a malicious user to gain full control of the affected system. For more information on this vulnerability, please refer to the following Microsoft page:

- Microsoft Security Bulletin MS04-011

It also attempts to log on to systems using a list of user names and passwords. It drops a copy of itself into accessible machines. This worm has backdoor capabilities. It executes commands sent in via Internet Relay Chat (IRC). It terminates certain antivirus processes and other security-related programs. It also modifies the Windows HOSTS file so that any access to specific antivirus Web sites is redirected to the local machine. This UPX-compressed worm runs on Windows NT, 2000, and XP.

WORM_AGOBOT.TD (Internet Worm): This memory-resident malware has both worm and backdoor capabilities. It drops itself as MSRV32.EXE in the Windows system folder and attempts to log on to systems using a list of user names and passwords. It opens a varied port and connects to an Internet Relay Chat (IRC) server. It then joins an IRC channel to receive malicious commands to be processed on a system. It also terminates antivirus-related programs and steals CD keys of certain game applications. This worm can also automatically notify the bot of systems affected by certain Microsoft Windows vulnerabilities. More information on the said vulnerabilities is available from the following Microsoft pages:

- Microsoft Security Bulletin MS03-026
- Microsoft Security Bulletin MS03-001
- Microsoft Security Bulletin MS03-007

It modifies the HOSTS file so that any access to certain antivirus and security Web sites is redirected to the local address 127.0.0.1. This malware runs on Windows NT, 2000, and XP.

WORM_CYCLE.A (Aliases: W32.Cycle, Win32.Cycle.A, W32/Cycle.worm.a) (Internet Worm): This worm exploits the Windows LSASS vulnerability, which is a buffer overrun that allows remote code execution and enables a malicious user to gain full control of the affected system. This vulnerability is discussed in detail in the following Web pages:

- MS04-011_MICROSOFT_WINDOWS
- Microsoft Security Bulletin MS04-011

It scans IP addresses and once it finds a vulnerable system, it drops a text file CYCLONE.TXT. The said text file contains a seemingly politically-tainted message. This worm also launches denial of service (DoS) attacks against specific Web sites, and terminates processes associated with other malware (such as SASSER worms and WORM_NETSKY.A). It runs on Windows ME, 2000, XP, and 2003.

WORM_MISODENE.A (Aliases: I-Worm.Famus, W32/Famus-A, W32/Misodene.a@MM virus, W32.Misodene@mm) (Internet Worm): This memory-resident worm propagates via e-mail with the following details:

- Subject: JENIFER DESNUDA\JENIFFER NAKED
- Attachment: www.jeniferlopez.com

It displays various fake error messages upon execution and drops a copy of itself using the file name WWW.JENIFERLOPEZ.COM in the Windows system folder. Its file dropper uses an Outlook Express icon to trick a user into executing it. It also uses a file name with long trailing spaces between the real file extension so that the user may not notice that the said file is actually an executable and not an Outlook mail message. An example is RefusedMail.eml<spaces>.exe. This malware is written in Visual Basic, a high-level programming language, and runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_MYDOOM.A (Aliases: Aliases: Win32:Mydoom [Wrm], W32/Mydoom.A@mm, Win32.HLLM.MyDoom.32768, Worm/MyDoom.A2, I-Worm.Win32.Mydoom.22528, W32.Novarg.A@mm, Win32/Mydoom.A@mm, I-Worm.Novarg, W32/Mydoom.A.worm, WORM_MIMAIL.R) (Internet Worm): This mass-mailing worm selects from a list of e-mail subjects, message bodies, and attachment file names for its e-mail messages. It spoofs the sender name of its messages so that they appear to have been sent by different users instead of the actual users on infected machines. It can also propagate through the KaZaA peer-to-peer file-sharing network. It performs a denial of service (DoS) attack against the software business site www.sco.com. It attacks the site if the system date is February 1, 2004 or later. It ceases attacking the site and running most of its routines on February 12, 2004. It runs a backdoor component, which it drops as the file SHIMGAPI.DLL. The backdoor component opens port 3127 to 3198 to allow remote users to access and manipulate infected systems. Note that it allows remote access even after February 12, 2004. This worm runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_NACHI.K (Aliases: Worm.Win32.Welchia.k, Win32/HLLW.Nachi.K) (Internet Worm): This worm can take advantage of the following vulnerabilities to propagate into accessible systems:

- RPC Locator vulnerability
- WebDAV vulnerability
- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- MS Workstation Service vulnerability

This worm also utilizes the backdoor functionalities of WORM_MYDOOM variants to propagate into infected systems although it also attempts to delete certain files and registry entries associated with some WORM_MYDOOM and WORM_DOOMJUICE variants. Moreover, it tries to patch the system against the RPC DCOM Buffer Overflow vulnerability. If the language version of the system is Japanese, it looks for certain files located in particular folders and overwrites them with an HTML code. It runs on Windows 2000 and XP.

WORM_SDBOT.BV (Internet Worm): This memory-resident malware has both worm and backdoor capabilities. It drops itself as CVMONITOR.EXE in the Windows system folder and attempts to log on to systems using a list of user names and passwords. It opens a varied port and acts as a server program controlled by an Internet Relay Chat (IRC) bot. It connects to an IRC server and joins an IRC channel to receive malicious commands. It also terminates antivirus-related programs and steals CD keys of certain game applications. This worm can also automatically notify the bot of systems affected by certain Microsoft Windows vulnerabilities. More information on the said vulnerabilities is available from the following Microsoft pages:

- Microsoft Security Bulletin MS03-026
- Microsoft Security Bulletin MS03-001
- Microsoft Security Bulletin MS03-007

It modifies the HOSTS file so that any access to certain antivirus and security Web sites is redirected to the local address 127.0.0.1. This malware runs on Windows NT, 2000, and XP.

WORM_SDBOT.ZG (Alias: Backdoor/Sdbot.Server) (Internet Worm): This worm scans the network and attempts to propagate by dropping a copy of itself into target machines. It uses the a list of text strings as user names and passwords to access a target system. This malware attempts to perform denial of service (DoS) attacks against the following Web sites:

- hayer.cjb.net
- hayerorg.com

It terminates processes related to antivirus and security utilities. It also steals the CD keys of several games. It runs on Windows 98, ME, NT, 2000 and XP.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *NOTE: At times, Trojans may contain names or content that may be considered offensive.*

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs and The WildList Organization International.

Trojan	Version	CyberNotes Issue #
Backdoor.Anyserv.B	B	SB04-119
Backdoor.Aphexdoor	N/A	CyberNotes-2004-03
Backdoor.Berbew.B	B	SB04-119
Backdoor.Berbew.D	D	SB04-119
Backdoor.Carool	**N/A**	**Current Issue**
Backdoor.Carufax.A	A	SB04-119
Backdoor.Cazno	N/A	SB04-091
Backdoor.Cazno.Kit	N/A	SB04-091
Backdoor.Danton	N/A	SB04-091
Backdoor.Domwis	N/A	CyberNotes-2004-04
Backdoor.Evivinc	N/A	SB04-119
Backdoor.Gaster	N/A	CyberNotes-2004-01

Trojan	Version	CyberNotes Issue #
Backdoor.Graybird.H	H	CyberNotes-2004-01
Backdoor.Graybird.I	I	SB04-119
Backdoor.IRC.Aimwin	N/A	SB04-105
Backdoor.IRC.Aladinz.F	F	CyberNotes-2004-01
Backdoor.IRC.Aladinz.G	G	CyberNotes-2004-02
Backdoor.IRC.Aladinz.H	H	CyberNotes-2004-02
Backdoor.IRC.Aladinz.J	J	CyberNotes-2004-04
Backdoor.IRC.Aladinz.L	L	CyberNotes-2004-05
Backdoor.IRC.Aladinz.M	M	CyberNotes-2004-05
Backdoor.IRC.Aladinz.N	N	SB04-105
Backdoor.IRC.Aladinz.O	O	SB04-105
Backdoor.IRC.Aladinz.P	P	SB04-119
Backdoor.IRC.Loonbot	N/A	CyberNotes-2004-05
Backdoor.IRC.Mutebot	N/A	SB04-105
Backdoor.IRC.MyPoo	N/A	SB04-091
Backdoor.IRC.MyPoo.Kit	N/A	SB04-091
Backdoor.IRC.Spybuzz	N/A	SB04-091
Backdoor.IRC.Zcrew.C	C	SB04-119
Backdoor.Kaitex.E	E	CyberNotes-2004-05
Backdoor.Medias	N/A	SB04-105
Backdoor.Mipsiv	**N/A**	**Current Issue**
Backdoor.NetCrack.B	B	SB04-119
Backdoor.Nibu.D	D	SB04-119
Backdoor.OptixPro.13.C	13.C	CyberNotes-2004-04
Backdoor.OptixPro.13b	13b	CyberNotes-2004-02
Backdoor.Portless	N/A	CyberNotes-2004-01
Backdoor.R3C.B	B	SB04-091
Backdoor.Ranky.E	E	SB04-091
Backdoor.Ranky.F	F	SB04-105
Backdoor.Sdbot.S	S	CyberNotes-2004-01
Backdoor.Sdbot.T	T	v
Backdoor.Sdbot.Y	Y	SB04-119
Backdoor.Sdbot.Z	**Z**	**Current Issue**
Backdoor.Sinups	**N/A**	**Current Issue**
Backdoor.Threadsys	N/A	CyberNotes-2004-02
Backdoor.Trodal	N/A	CyberNotes-2004-01
Backdoor.Tumag	N/A	SB04-091
Backdoor.Tuxder	N/A	CyberNotes-2004-02
BackDoor-AWQ.b	B	CyberNotes-2004-01
BackDoor-CBA	**CBA**	**Current Issue**
BackDoor-CBH	N/A	CyberNotes-2004-01
BackDoor-CCT	CCT	SB04-119
BDS/Purisca	N/A	CyberNotes-2004-01
BKDR_SPYBOT.ZA	**ZA**	**Current Issue**
BKDR_UPROOTKIT.A	A	CyberNotes-2004-01
DDoS-Chessmess	**N/A**	**Current Issue**
Dial/ExDial-A	A	CyberNotes-2004-01
DOS_MASSMSG.A	A	CyberNotes-2004-01
Download.Berbew.dam	N/A	CyberNotes-2004-01
Download.Chamber	N/A	SB04-091
Download.Chamber.Kit	N/A	SB04-091
Download.SmallWeb	N/A	SB04-091
Download.SmallWeb.Kit	N/A	SB04-091
Download.Tagdoor	N/A	SB04-105
Downloader.Botten	N/A	CyberNotes-2004-05
Downloader.Mimail.B	B	CyberNotes-2004-02
Downloader.Psyme	N/A	SB04-105
Downloader-GD	GD	CyberNotes-2004-01

Trojan	Version	CyberNotes Issue #
Downloader-GH	GH	CyberNotes-2004-02
Downloader-GN	GN	CyberNotes-2004-02
Downloader-IU	IU	SB04-105
Dyfuca	N/A	CyberNotes-2004-01
Exploit-URLSpoof	N/A	CyberNotes-2004-01
Hacktool.Sagic	N/A	CyberNotes-2004-01
IRC-Bun	N/A	CyberNotes-2004-01
Java.StartPage	N/A	CyberNotes-2004-05
JS/AdClicker-AB	AB	CyberNotes-2004-01
Keylogger.Stawin	N/A	CyberNotes-2004-03
Keylog-Ramb	N/A	SB04-119
MAC_MP3CONCEPT.A	A	SB04-119
MultiDropper-GP.dr	GP.dr	CyberNotes-2004-04
MultiDropper-JW	JW	SB04-091
Needy.C	C	CyberNotes-2004-03
Needy.D	D	SB04-105
Needy.E	E	SB04-105
Needy.F	F	SB04-105
Needy.G	G	SB04-105
Needy.H	H	SB04-105
Needy.I	I	SB04-105
Ouch	N/A	CyberNotes-2004-02
Perl/Exploit-Sqlinject	N/A	CyberNotes-2004-01
Phish-Potpor	N/A	CyberNotes-2004-04
Proxy-Agent	N/A	CyberNotes-2004-03
Proxy-Cidra	N/A	CyberNotes-2004-01
PWS-Datei	N/A	CyberNotes-2004-01
PWSteal.Bancos.D	D	CyberNotes-2004-01
PWSteal.Bancos.E	E	CyberNotes-2004-05
PWSteal.Bancos.F	F	SB04-091
PWSteal.Bancos.G	G	SB04-091
PWSteal.Bancos.H	H	SB04-119
PWSteal.Banpaes.C	C	CyberNotes-2004-05
PWSteal.Freemega	N/A	CyberNotes-2004-02
PWSteal.Goldpay	N/A	SB04-105
PWSteal.Irftp	N/A	CyberNotes-2004-05
PWSteal.Lemir.G	G	SB04-105
PWSteal.Leox	N/A	CyberNotes-2004-02
PWSteal.Olbaid	N/A	CyberNotes-2004-03
PWSteal.Sagic	N/A	CyberNotes-2004-01
PWSteal.Souljet	N/A	SB04-105
PWSteal.Tarno.B	B	CyberNotes-2004-05
PWSteal.Tarno.C	C	SB04-091
PWSteal.Tarno.E	E	SB04-119
QReg-9	9	CyberNotes-2004-04
Rahitor	**N/A**	**Current Issue**
Spy-Peep	N/A	SB04-091
Startpage-AI	AI	CyberNotes-2004-01
StartPage-AU	AU	CyberNotes-2004-02
StartPage-AX	AX	CyberNotes-2004-02
TR/DL906e	N/A	CyberNotes-2004-01
TR/Psyme.B	B	CyberNotes-2004-01
Troj/AdClick-Y	Y	CyberNotes-2004-03
Troj/Adtoda-A	**A**	**Current Issue**
Troj/Adtoda-A	A	SB04-105
Troj/Agent-C	C	CyberNotes-2004-01
Troj/Agobot-HZ	**HZ**	**Current Issue**
Troj/Agobot-IB	**IB**	**Current Issue**

Trojan	Version	CyberNotes Issue #
Troj/Antikl-Dam	N/A	CyberNotes-2004-01
Troj/Apher-L	L	CyberNotes-2004-02
Troj/Badparty-A	A	SB04-091
Troj/Banker-S	S	SB04-119
Troj/Bdoor-CCK	CCK	CyberNotes-2004-05
Troj/BeastDo-M	M	CyberNotes-2004-01
Troj/BeastDo-N	N	CyberNotes-2004-01
Troj/ByteVeri-E	E	CyberNotes-2004-03
Troj/Chapter-A	A	CyberNotes-2004-03
Troj/Cidra-A	A	CyberNotes-2004-01
Troj/Cidra-D	D	CyberNotes-2004-05
Troj/Control-E	E	CyberNotes-2004-03
Troj/CoreFloo-D	D	CyberNotes-2004-01
Troj/Daemoni-B	B	CyberNotes-2004-03
Troj/Daemoni-C	C	CyberNotes-2004-03
Troj/Darium-A	A	CyberNotes-2004-01
Troj/DDosSmal-B	B	CyberNotes-2004-04
Troj/DDosSmal-B	B	SB04-119
Troj/Delf-JV	JV	CyberNotes-2004-02
Troj/Delf-NJ	NJ	CyberNotes-2004-01
Troj/DelShare-G	G	CyberNotes-2004-01
Troj/Digits-B	B	CyberNotes-2004-03
Troj/Divix-A	A	CyberNotes-2004-02
Troj/Dloader-K	K	CyberNotes-2004-01
Troj/Domwis-A	A	CyberNotes-2004-05
Troj/Eyeveg-C	C	CyberNotes-2004-05
Troj/Femad-B	B	CyberNotes-2004-03
Troj/Femad-D	D	CyberNotes-2004-01
Troj/Flator-A	A	CyberNotes-2004-01
Troj/Flood-CR	CR	CyberNotes-2004-02
Troj/Flood-DZ	DZ	CyberNotes-2004-03
Troj/Getdial-A	A	CyberNotes-2004-01
Troj/HacDef-100	100	CyberNotes-2004-05
Troj/Hackarmy-A	A	CyberNotes-2004-02
Troj/Hidemirc-A	A	CyberNotes-2004-03
Troj/Hosts-A	A	CyberNotes-2004-01
Troj/Hosts-B	B	CyberNotes-2004-02
Troj/IEStart-G	G	CyberNotes-2004-02
Troj/Inor-B	B	CyberNotes-2004-02
Troj/Ipons-A	A	CyberNotes-2004-01
Troj/Ircbot-S	S	CyberNotes-2004-02
Troj/IRCBot-U	U	CyberNotes-2004-03
Troj/Ircfloo-A	A	CyberNotes-2004-03
Troj/JDownL-A	A	SB04-105
Troj/Ketch-A	A	CyberNotes-2004-01
Troj/Kuzey-A	A	CyberNotes-2004-02
Troj/Lalus-A	A	CyberNotes-2004-01
Troj/Ldpinch-C	C	CyberNotes-2004-02
Troj/LDPinch-G	G	CyberNotes-2004-05
Troj/LDPinch-H	H	CyberNotes-2004-05
Troj/LdPinch-L	L	SB04-119
Troj/Legmir-E	E	CyberNotes-2004-01
Troj/Legmir-K	K	SB04-119
Troj/Lindoor-A	A	CyberNotes-2004-02
Troj/Linploit-A	A	CyberNotes-2004-02
Troj/Loony-E	E	SB04-119
Troj/Mahru-A	A	CyberNotes-2004-03
Troj/Mircsend-A	A	CyberNotes-2004-02

Trojan	Version	CyberNotes Issue #
Troj/Mmdload-A	A	CyberNotes-2004-02
Troj/MsnCrash-B	B	CyberNotes-2004-01
Troj/Mssvc-A	A	CyberNotes-2004-01
Troj/Myss-C	C	CyberNotes-2004-04
Troj/Narhem-A	A	CyberNotes-2004-05
Troj/NoCheat-B	B	CyberNotes-2004-03
Troj/Noshare-K	K	CyberNotes-2004-02
Troj/Pinbol-A	A	CyberNotes-2004-04
Troj/Prorat-D	D	SB04-091
Troj/Proxin-A	A	CyberNotes-2004-02
Troj/Psyme-U	**U**	**Current Issue**
Troj/Ranckbot-A	A	SB04-091
Troj/Ranck-K	K	CyberNotes-2004-05
Troj/Rybot-A	A	SB04-105
Troj/Saye-A	A	CyberNotes-2004-02
Troj/Sdbot-AP	AP	CyberNotes-2004-03
Troj/SdBot-BB	BB	CyberNotes-2004-02
Troj/Sdbot-CY	CY	CyberNotes-2004-01
Troj/Sdbot-EF	EF	CyberNotes-2004-01
Troj/SdBot-EG	EG	CyberNotes-2004-01
Troj/SdBot-EI	EI	CyberNotes-2004-01
Troj/Sdbot-EJ	EJ	CyberNotes-2004-02
Troj/Sdbot-EK	EK	CyberNotes-2004-02
Troj/Sdbot-EL	EL	CyberNotes-2004-02
Troj/Sdbot-FM	FM	CyberNotes-2004-04
Troj/Search-A	A	CyberNotes-2004-02
Troj/Sect-A	A	CyberNotes-2004-02
Troj/Seeker-F	F	CyberNotes-2004-01
Troj/Small-AG	AG	SB04-119
Troj/Small-AW	AW	CyberNotes-2004-03
Troj/Spooner-C	C	CyberNotes-2004-02
Troj/SpyBot-AA	AA	CyberNotes-2004-01
Troj/Spybot-AM	AM	CyberNotes-2004-01
Troj/Spybot-C	C	CyberNotes-2004-01
Troj/StartPa-AE	AE	SB04-119
Troj/StartPag-C	C	CyberNotes-2004-01
Troj/StartPag-E	E	CyberNotes-2004-02
Troj/StartPg-AU	AU	CyberNotes-2004-01
Troj/StartPg-AY	AY	CyberNotes-2004-01
Troj/StartPg-BG	BG	CyberNotes-2004-01
Troj/StartPg-U	U	CyberNotes-2004-01
Troj/Stawin-A	A	CyberNotes-2004-03
Troj/TCXMedi-E	E	CyberNotes-2004-01
Troj/Tofger-F	F	CyberNotes-2004-01
Troj/Tofger-L	L	CyberNotes-2004-01
Troj/Troll-A	A	CyberNotes-2004-02
Troj/Uproot-A	A	CyberNotes-2004-01
Troj/Volver-A	A	CyberNotes-2004-03
Troj/Weasyw-A	A	CyberNotes-2004-02
Troj/Webber-D	D	CyberNotes-2004-01
Troj/Webber-H	H	SB04-119
Troj/Winpup-C	C	CyberNotes-2004-03
Trojan.Adwaheck	**N/A**	**Current Issue**
Trojan.Anymail	N/A	CyberNotes-2004-01
Trojan.AphexLace.Kit	N/A	SB04-105
Trojan.Bansap	N/A	CyberNotes-2004-04
Trojan.Bookmarker	N/A	CyberNotes-2004-01
Trojan.Bookmarker.B	B	CyberNotes-2004-02

Trojan	Version	CyberNotes Issue #
Trojan.Bookmarker.C	C	CyberNotes-2004-02
Trojan.Bookmarker.D	C	CyberNotes-2004-03
Trojan.Bookmarker.E	E	CyberNotes-2004-03
Trojan.Bookmarker.F	F	CyberNotes-2004-05
Trojan.Bookmarker.G	G	SB04-091
Trojan.Brutecode	N/A	SB04-105
Trojan.Cookrar	N/A	SB04-105
Trojan.Download.Revir	N/A	CyberNotes-2004-01
Trojan.Dustbunny	N/A	SB04-091
Trojan.Etsur	N/A	CyberNotes-2004-05
Trojan.Gema	N/A	CyberNotes-2004-01
Trojan.Gipma	N/A	CyberNotes-2004-05
Trojan.Gutta	N/A	CyberNotes-2004-04
Trojan.Httpdos	N/A	CyberNotes-2004-02
Trojan.KillAV.D	D	SB04-091
Trojan.Linst	N/A	SB04-091
Trojan.Lyndkrew	N/A	SB04-105
Trojan.Mercurycas.A	A	SB04-119
Trojan.Mitglieder.C	C	CyberNotes-2004-02
Trojan.Mitglieder.D	D	CyberNotes-2004-05
Trojan.Mitglieder.E	E	CyberNotes-2004-05
Trojan.Mitglieder.F	F	SB04-105
Trojan.Mitglieder.H	H	SB04-119
Trojan.Mitglieder.I	I	SB04-119
Trojan.Noupdate	N/A	CyberNotes-2004-05
Trojan.Noupdate.B	B	SB04-091
Trojan.Popdis	N/A	SB04-119
Trojan.PWS.Qphook	N/A	CyberNotes-2004-01
Trojan.PWS.QQPass.F	F	CyberNotes-2004-04
Trojan.Regsys	N/A	SB04-091
Trojan.Simcss.B	B	CyberNotes-2004-05
Trojan.Tilser	N/A	CyberNotes-2004-05
Trojan.Trunlow	N/A	SB04-105
Unix/Exploit-SSHIDEN	N/A	CyberNotes-2004-02
UrlSpoof.E	E	CyberNotes-2004-03
VBS.Bootconf.B	B	CyberNotes-2004-04
VBS.Shania	N/A	CyberNotes-2004-03
VBS/Inor-C	C	CyberNotes-2004-03
VBS/Suzer-B	B	CyberNotes-2004-01
VBS/Wisis-A	A	CyberNotes-2004-02
W32.Bizten	N/A	CyberNotes-2004-01
W32.Dumaru.AI	AI	SB04-119
W32.Hostidel.Trojan.B	B	CyberNotes-2004-03
W32.Kifer	N/A	CyberNotes-2004-04
W32.Kifer.B	B	CyberNotes-2004-04
W32.Netad.Trojan	**N/A**	**Current Issue**
W32.Tuoba.Trojan	N/A	SB04-091
Xombe	N/A	CyberNotes-2004-01

Backdoor.Carool: This is a Backdoor Trojan horse that allows unauthorized remote access your computer. The Trojan also installs a keylogger and steals cached passwords.

BackDoor-CBA: When run this Trojan installs itself in the "Run" key as SCHECK to be loaded on next restart. On initial installation the backdoor attempts to connect to lost.updateserver1.com to download a php script which provides commands for the backdoor including which backdoor port to open for listening on.

Backdoor.Mipsiv: This is a Trojan horse that connects to an IRC server and allows a malicious user to perform keylogging and network scanning functions. When Backdoor.Mipsiv is executed, it copies itself as %System%\mpisvc.exe and adds the value, "MapiDrv" = "%System%\mpisvc.exe," to the registry keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

The Trojan attempts to connect to a predetermined IRC server and channel on TCP port 443. It awaits commands from a malicious user.

Backdoor.Sdbot.Z (Alias: Backdoor.SdBot.ht): This is a Trojan horse that can be controlled using IRC. The existence of the file wupdated.exe is an indication of a possible infection. When Backdoor.Sdbot.Z runs, it copies itself as %System%\Wupdated.exe. The Trojan creates a service named "Windows Update Service." The service runs %System%\Wupdated.exe. It also attempts to delete the value "Configuration Loaded" from the registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

Backdoor.Sinups: This is an ASP and a VBScript-based Backdoor Trojan horse. This Trojan gives a malicious user full control of a computer that runs a Microsoft IIS Web server. The Trojan gives the malicious user a Web-based interface on an infected system, from which the malicious user can perform a variety of actions on the system (see the "Technical Details" section for the list of actions).

BKDR_SPYBOT.ZA: This malware is usually downloaded from a particular FTP (File Transfer Protocol) site by the malicious batch file detected as BAT_SPYBOT.ZA. Similar to its earlier variants, this malware has the following capabilities:

- Terminate processes
- Log keystrokes
- Execute programs
- Obtain names of active windows/dialog boxes
- Create/remove directories
- Scan ports
- Join/quit a channel
- Join/quit an IRC server
- Redirect packet from one port to another
- Send raw message
- List all running processes

DDoS-Chessmess: This is a simple Trojan that spams message boxes via the Microsoft Windows Messenger Service. The program pretends to be a chess game, using an icon and when run, it broadcasts a message.

Rahitor (Alias: TrojanDownloader.Win32.Rahitor): This is a Trojan downloader that downloads and installs a spying Trojan named Agent.K on a computer from the virtumonde.com website. The Trojan's file is downloaded into Windows directory and then activated. The downloader avoids downloading if the host's name contains 'mil' or 'gov' strings.

Troj/Adtoda-A: This is a backdoor Trojan. When first run, Troj/Adtoda-A will display the following two messages: "Setup was not able to continue the installation. An illegal copy of Windows Operating System was detected on this computer. The computer information's is already collect and will be post as this computer name: (name of machine)" and "The operating system will not work properly before you get a permission after you complete the penalty! For any detail information, Please contact the following link:

- http:\\www.microsoft.com\~msproduct\~watch\~piracy10\secureID=OS_wiNver_532Fg32_ap12nt04A"

After the user clicks "OK" on both of these messages, Troj/Adtoda-A installs itself and activates the payload. This inverts the screen and freezes the machine so that is needs to be rebooted. In order to run automatically when Windows starts up the Trojan creates the file:

- C:\Windows\system\winupd32.exe and the shortcut
- C:\Windows\Start Menu\Programs\StartUp\System Update Service.lnk pointing to it.

These files will cause the payload to be run again on system boot. Troj/Adtoda-A also attempts to modify C:\boot.ini to prevent debugging.

Troj/Agobot-HZ (Aliases: W32.Gaobot.AFJ, W32/Gaobot.worm.gen.j virus, INFECTED Backdoor.Agobot.gen): This is a backdoor Trojan for the Windows platform. It allows a malicious user remote access to an infected computer. In order to run automatically when Windows starts up Troj/Agobot-HZ creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\File System Service=wmiprvsc.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\File SystemService=wmiprvsc.exe.

Troj/Agobot-IB (Aliases: Backdoor.Agobot.gen, W32/Gaobot.worm.gen.j, W32.Gaobot.AFJ, WORM_AGOBOT.JH): This is a backdoor Trojan for the Windows platform. It allows a malicious user remote access to an infected computer. In order to run automatically when Windows starts up Troj/Agobot-IB creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Update=Microsoft.exe
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Microsoft Update=Microsoft.exe.

Troj/Psyme-U (Alias: TojanDownloader.VBS.Psyme.t) This is a HTML based script which exploits the ADODB stream vulnerability associated with Microsoft Internet Explorer to download and run executables.

Trojan.Adwaheck: This is a Trojan horse that contains both Adware and backdoor Trojan functionality. When Trojan.Adwaheck runs, it creates the value, "%Trojan_filename_without_extension%"="%Trojan_filename%," in the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. The Trojan extracts and decrypts a VBScript from its body, patches it with additional code, which initializes several internal variables, and then runs that script. It also attempts to insert its own marker into the displayed HTML pages. Trojan Adwaheck searches for open Web browser windows and inspects the opened Web sites. If it detects one of the following strings among the browsed URLs:

- google.com
- yahoo.com
- search.msn.com
- s.teoma.com
- search.aol.com
- altavista.com
- web.ask.com
- msxml.infospace.com/home/search

it will attempt to redirect the search requests to the links that are hard-coded in the Trojan. The Trojan submits a request to a remote Web site and parses the reply. The reply may contain backdoor commands that allow the Trojan to query the hard-coded URLs and check whether an updated version is available. If there is a new version available, Trojan.Adwaheck will retrieve it, save it using the file name contained in the backdoor command, and then run it. The backdoor functionality also allows it to manage the redirection of the requested URLs.

W32.Netad.Trojan: This is a Trojan horse that attempts to delete all the files on the C: drive. It is written in the Delphi programming language.